(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2001年3月15日 (15.03.2001)

PCT

(10) 国際公開番号
WO 01/18772 A1

(51) 国際特許分類[6]: G09C 1/00, H04L 9/30

(21) 国際出願番号: PCT/JP99/04869

(22) 国際出願日: 1999年9月8日 (08.09.1999)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(71) 出願人 (米国を除く全ての指定国について): 株式会社 日立製作所 (HITACHI, LTD.) [JP/JP]; 〒101-8010 東京都千代田区神田駿河台四丁目6番地 Tokyo (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 桶屋勝幸 (OKEYA, Katsuyuki) [JP/JP]; 〒244-8555 神奈川県横浜市戸塚区戸塚町5030番地 株式会社 日立製作所 ソフトウェア事業部内 Kanagawa (JP).

(74) 代理人: 弁理士 作田康夫(SAKUTA, Yasuo); 〒100-8220 東京都千代田区丸の内一丁目5番1号 株式会社 日立製作所内 Tokyo (JP).

(81) 指定国 (国内): CA, JP, US.

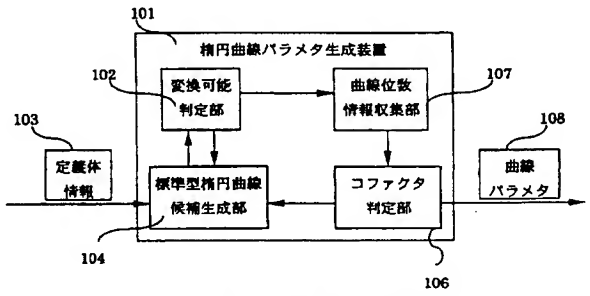
(84) 指定国 (広域): ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(54) Title: ELLIPTIC CURVE GENERATING METHOD AND DEVICE, ELLIPTIC ENCRYPTION SYSTEM AND RECORDING MEDIUM

(54) 発明の名称: 楕円曲線生成方法 装置及び楕円暗号システム並びに記録媒体




101 ... ELLIPTIC CURVE PARAMETER GENERATING DEVICE
102 ... CONVERSION POSSIBILITY DECISION UNIT
103 ... DEFINITION OBJECT INFORMATION
104 ... STANDARD ELLIPTIC CURVE CANDIDATE GENERATING UNIT
106 ... COFACTOR DECISION UNIT
107 ... CURVE ORDER INFORMATION GATHERING UNIT
108 ... CURVE PARAMETER

(57) Abstract: A method and device for generating a safe standard elliptic curve that can be converted into a Montgomery elliptic curve, an elliptic encryption system and a recording medium, wherein a curve parameter generating device is constituted which gives a decision condition under which a curve order-related condition is separated from a decision condition whether or not a standard elliptic curve can be converted into a Montgomery elliptic curve and which incorporates a conversion possibility decision unit. For a method of generating a curve having a cofactor of 4, a condition under which a curve order can be divided by 8 is given.

[続葉有]

WO 01/18772 A1

(57) 要約:

本発明の目的は、モンゴメリ型楕円曲線に変換可能であり且つ安全な標準型楕円曲線の生成方法、装置及び楕円暗号システム並びに記録媒体を提供することにある。

この目的を達成するために、標準型楕円曲線がモンゴメリ型楕円曲線に変換可能かの判定条件から曲線位数に関する条件を切り離した判定条件を与え、変換可能判定部を組み込んだ曲線パラメタ生成装置を構成する。また、コファクタが４である曲線の生成方法に関しては、曲線位数が８で割れる条件を与える。

# 明 細 書

## 楕円曲線生成方法、装置及び楕円暗号システム並びに記録媒体

### 技術分野

本発明はコンピュータネットワークにおけるセキュリティ技術に係り、特に楕円暗号において用いる楕円曲線の生成方法、楕円曲線の装置及び楕円暗号システム並びにその方法を格納した記録媒体に関する。

### 背景技術

楕円暗号において用いる楕円曲線として、標準型楕円曲線$y^2 = f(x)$、ただし$f(x) = x^3 + ax + b \quad (a,b \in F_p)$、$F_p$は要素数が$p$個の有限体で$p$は大きな素数、を用いることがある。$y_0^2 = f(x_0)$をみたす$(x_0,y_0)$の組$(x_0,y_0 \in F_p)$を曲線上の点といい、それら点全体に無限遠点を付け加えた集合に演算を入れることができ、その点の個数を曲線位数という。曲線位数を$n$として$n = cl$と正整数$c$と大きな素数$l$と表した時、$c$をコファクタといい、$c$の値が小さい時にその楕円曲線を安全という。安全な標準型楕円曲線の生成方法として、ランダムに標準型楕円曲線を生成しその曲線位数により安全性を判定し、安全となるまで標準型楕円曲線の再生成を行う方法が ANSI X9.62, Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm(ECDSA), (1999)に記載されている。

また、モンゴメリ型楕円曲線$BY^2 = X^3 + AX^2 + X \quad (A,B \in F_p)$を用いると標準型楕円曲線よりも高速に演算を実行できることが P.L.Montgomery, Speeding the Pollard and Elliptic Curve

Methods of Factorization, Math. Comp. 48 (1987) 243-264. に記載されている。標準型楕円曲線がモンゴメリ型楕円曲線に変換可能とは、標準型楕円曲線上の点とモンゴメリ型楕円曲線上の点とが１対１に対応し、それぞれにおける演算が一致することをいう。全ての標準型楕円曲線がモンゴメリ型楕円曲線に変換可能であるわけではない。伊豆哲也氏による「楕円曲線暗号演算の計算方法について」１９９９年暗号と情報セキュリティシンポジウム予稿集 vol. 1, (1999) 275-280. には標準型楕円曲線からモンゴメリ型楕円曲線への変換が可能なための条件が記載されている。さらにモンゴメリ型楕円曲線の曲線位数が必ず４で割れることも上記資料に記載されている。

上記従来技術はモンゴメリ型楕円曲線に変換可能な標準型楕円曲線の生成に関しては考慮されていなかった。そのためにモンゴメリ型楕円曲線に変換可能であり且つ安全な標準型楕円曲線の生成のためには、安全な標準型楕円曲線を生成した後に、それがモンゴメリ型楕円曲線に変換可能かどうかを判定し、変換不可能であれば安全な標準型楕円曲線を再生成し、変換可能となるまで繰り返すといった手順を踏まなければならなかった。一般的に、安全な標準型楕円曲線を生成する処理は、モンゴメリ型楕円曲線に変換可能かどうかを判定する処理より時間を要する。そのため上記性質を持った楕円曲線の生成には多大な時間を必要とし、ネットワークセキュリティを確保するための楕円暗号において、定期的に使用している楕円曲線を上記性質を持った新しい楕円曲線に置き換えることは難しかった。ここで、公開鍵を知らなくても楕円曲線のみを知っていれば攻撃のための前計算を行なえる攻撃法（Baby-Step-Giant-Step 法）に対しては、楕円曲線を定期的に新しいものに置き換える以外に安全性を保つ方法は存在しないと言われている。したがって、従来技術を用いた場合は、特定楕円曲線に対する攻撃を受け易い状態に

あった。

本発明の目的は演算の高速性及び安全性を向上させる楕円曲線生成方法、装置及び楕円暗号システム並びに記録媒体を提供することにある。

発明の開示

上記目的は、楕円曲線の生成方法であって、第１の楕円曲線（例えば、$y^2=x^3+ax+b$ ）を生成するステップと、前記第１の楕円曲線が第２の楕円曲線（例えば、$BY^2=X^3+AX^2+X$ ）に変換可能であるかを判定するステップと、前記第２の楕円曲線に変換可能な第１の楕円曲線の安全性を判定するステップとを有することにより達成する。ここで第１の楕円曲線は、予め定められた素数位数の体上定義された第１の楕円曲線を用いても良い。また、前記第２の楕円曲線に変換可能であるかを判定するステップは、前記第１の楕円曲線 $y^2=f(x)=x^3+ax+b$ に対して、$f(\alpha)=0$ となる $\alpha$ が存在するかを判定するステップと、$f(\alpha)=0$ となる $\alpha$ に対して $f'(\alpha)$ が平方根を持つかを判定するステップとからなることにより達成する。また、前記第１の楕円曲線の安全性を判定するステップは、前記第１の楕円曲線の曲線位数に関する情報を抽出するステップと、前記曲線位数に関する情報からコファクタの判定を行うステップとを有することにより達成する。また、第１の楕円曲線 $y^2=x^3+ax+b$ と第２の楕円曲線 $y^2=x^3+ar^2x+br^3$ とを生成するステップと、前記第１の楕円曲線が第３の楕円曲線 $BY^2=X^3+AX^2+X$ に変換可能であるかを判定するステップと、前記第１の楕円曲線が前記第３の楕円曲線に変換可能である場合、前記第１の楕円曲線及び前記第２の楕円曲線の安全性を判定するステップとを有することにより達成する。また、楕円暗号における素体上定義された楕円曲線の生成方法であって、ランダムな標準型楕円曲線 $y^2=x^3$

＋ａｘ＋ｂを生成するステップと、前記生成された標準型楕円曲線$y^2=x^3+ax+b$がモンゴメリ型楕円曲線$BY^2=X^3+AX^2+X$に変換可能であるかを判定するステップと、前記楕円曲線の曲線位数の８による整除性を判定するステップと、前記楕円曲線の曲線位数に関する情報を収集するステップと、前記曲線位数の情報からコファクタの値を判定するステップとからなり、モンゴメリ型楕円曲線に変換可能であり且つコファクタが４である標準型楕円曲線を生成することにより達成する。

また、楕円曲線生成装置であって、第１の楕円曲線$y^2=x^3+ax+b$を生成する楕円曲線候補生成部と、前記第１の楕円曲線が第２の楕円曲線$BY^2=X^3+AX^2+X$に変換可能であるかを判定する変換可能判定部と、前記第２の楕円曲線に変換可能な第１の楕円曲線の安全性を判定する安全性判定部とを備えたことにより達成する。ここで、前記変換可能判定部は、前記第１の楕円曲線に対して、ｆ（$\alpha$）＝０となる$\alpha$が存在するかを判定する根存在判定部と、ｆ（$\alpha$）＝０となる$\alpha$に対してｆ‘（$\alpha$）が平方根を持つかを判定する平方根判定部とからなることにより達成する。また、前記変換可能判定部は、前記第１の楕円曲線に対して、ｆ（$\alpha$）＝０となる$\alpha$が存在するかを判定する根存在判定部と、ｆ（$\alpha$）＝０となる$\alpha$に対してｆ‘（$\alpha$）が平方剰余であるかを判定する平方剰余判定部とからなることにより達成する。また、第１の計算機と第２の計算機との間で暗号化通信を行う暗号システムで使用される楕円曲線生成装置であって、前記計算機から楕円曲線の生成要請を受け、モンゴメリ型楕円曲線に変換可能な標準型楕円曲線を生成することにより達成する。

また、楕円暗号を利用して暗号化通信を行う暗号システムであって、暗号化通信を受信する第１の計算機と、暗号化通信を送信する第２の計算機と、前記第１の計算機から楕円曲線の生成要請を受けて、モンゴメ

リ型楕円曲線に変換可能な標準型楕円曲線を生成する楕円曲線生成装置とを備えたことにより達成する。また、暗号化通信に使用している楕円曲線に置換の必要性があるか否かを管理する曲線置換管理装置を更に備え、前記楕円曲線に置換の必要性が生じた場合は、前記楕円曲線生成装置が新たに生成した楕円曲線に置換して暗号化通信を行うことにより達成する。尚、上記目的を達成するためには、上述した方法、装置及びシステムで実現している機能を実現するプログラムを格納した記録媒体であっても良い。

図面の簡単な説明

第１図は、本発明の第１実施例において楕円暗号システムにおける曲線パラメタ生成サーバ内での楕円曲線の生成方法及び装置における処理の流れを示す図である。第２図は、本発明の第１実施例を示す楕円曲線の生成方法及び装置におけるモンゴメリ型楕円曲線に変換可能であり且つ安全な標準型楕円曲線の生成方法を示すフローチャートである。第３図は、本発明の楕円曲線の生成方法及び装置内の変換可能判定部における標準型楕円曲線からモンゴメリ型楕円曲線に変換可能かの判定方法を示すフローチャートである。第４図は、本発明の第１、２実施例の応用例を示す楕円曲線の生成方法及び装置におけるモンゴメリ型楕円曲線に変換可能であり且つ安全な標準型楕円曲線の生成方法を示すフローチャートである。第５図は、本発明の第２実施例の楕円暗号システムにおける曲線パラメタ生成サーバ内での楕円曲線の生成方法及び装置における処理の流れを示す図である。第６図は、本発明の第２実施例を示す楕円曲線の生成方法及び装置におけるモンゴメリ型楕円曲線に変換可能であり且つコファクタが４である標準型楕円曲線の生成方法を示すフローチャートである。第７図は、本発明の第２実施例における楕円曲線

パラメタ生成装置内でのモンゴメリ型楕円曲線に変換可能な標準型楕円曲線の曲線位数に対する８による整除性の判定方法を示すフローチャートである。特に、定義体素数が４を法として１の場合の判定方法を示している。第８図は、本発明の第２実施例における楕円曲線パラメタ生成装置内でのモンゴメリ型楕円曲線に変換可能な標準型楕円曲線の曲線位数に対する８による整除性の判定方法を示すフローチャートである。特に定義体素数が４を法として３の場合の判定方法を示している。第９図は、本発明の第２実施例で８による整除性の判定のための条件を列挙している表である。第１０図は、本発明の第３実施例の楕円暗号システムにおける曲線パラメタ生成サーバ内での楕円曲線の生成方法及び装置における処理の流れを示す図である。第１１図は、本発明の第３実施例を示す楕円曲線の生成方法及び装置におけるモンゴメリ型楕円曲線に変換可能であり且つコファクタが４である標準型楕円曲線の生成方法を示すフローチャートである。第１２図は、本発明の第３実施例における標準型楕円曲線に対する適当性判定方法を示すフローチャートである。特に、定義体素数が４を法として１の場合の判定方法を示している。第１３図は、本発明の第３実施例における標準型楕円曲線に対する適当性判定方法を示すフローチャートである。特に定義体素数が４を法として３の場合の判定方法を示している。第１４図は、本発明の楕円暗号システムの一例の構成図である。第１５図は、本発明の第４実施例における楕円暗号システムでの曲線生成方法に関するフローチャートである。第１６図は、本発明の第５実施例における楕円暗号システムの構成図である。第１７図は、本発明の第５実施例における楕円暗号システムでの曲線生成方法に関するフローチャートである。第１８図は、本発明の第６実施例における楕円暗号システムの構成図である。第１９図は、本発明の第６実施例における楕円暗号システムでの曲線生成方法に関するフロー

チャートである。第２０図は、本発明の第７実施例における楕円暗号システムの構成図である。第２１図は、本発明の第７実施例における楕円暗号システムでの曲線生成方法に関するフローチャートである。第２２図は、楕円曲線パラメタ生成装置内での標準型楕円曲線からモンゴメリ型楕円曲線への変換判定方法及び装置における処理の流れを示す図である。第２３図は、本発明の楕円暗号システムにおける曲線パラメタ変換装置での標準型楕円曲線からモンゴメリ型楕円曲線への変換における処理の流れを示す図である。第２４図は、曲線パラメタ変換方法を示すフローチャートである。第２５図は、本発明の楕円曲線パラメタ生成装置内での標準型楕円曲線からモンゴメリ型楕円曲線への変換可能判定方法及び装置における処理の流れを示す図である。第２６図は、標準型楕円曲線からモンゴメリ型楕円曲線への変換可能判定方法を示すフローチャートである。第２７図は、本発明の実施例におけるデータ構造である。第２８図は、曲線置換管理装置の一実施例を示す図である。第２９図は、曲線置換管理装置を公開鍵サーバに組み込んだ楕円暗号システムでの曲線パラメタ置換における処理の流れを示すシーケンス図である。

発明を実施するための最良の形態

以下、本発明の一実施例を図面により説明する。図１４は本発明が適用される楕円暗号システムの構成図の一例である。

まず、楕円曲線暗号システムを構成する曲線パラメタ生成サーバ内の楕円曲線パラメタ生成装置について図１、図２を用いて説明する。図１は楕円暗号システムにおける曲線パラメタ生成サーバ内でのモンゴメリ型楕円曲線に変換可能であり且つ安全な標準型楕円曲線の生成方法の第１実施例を示す図である。図２は第１実施例の楕円曲線パラメタ生成装置１０１における標準型楕円曲線の曲線パラメタの生成方法を示すフ

ローチャートである。

楕円曲線パラメタ生成装置１０１では、定義体情報１０３を入力し、以下の手順により曲線パラメタ１０８を出力する。ここで定義体情報１０３は図２７における、定義体のビット長を含んだ定義体情報２７０１もしくは定義体素数を含んだ定義体情報２７０４で与えられている。楕円曲線候補生成部１０４において、定義体情報１０３よりランダムな標準型楕円曲線を生成する（ステップ２０１）。ランダムな標準型楕円曲線の生成方法については ANSI X9.62, Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm(ECDSA), (1999)に記述されている。変換可能判定部１０２において楕円曲線候補生成部１０４で生成された標準型楕円曲線がモンゴメリ型楕円曲線に変換可能かの判定を行なう（ステップ２０２）。変換不可能であれば楕円曲線候補生成部１０４で標準型楕円曲線の再生成を行ない、変換可能となるまで繰り返す。曲線位数情報収集部１０７では変換可能判定部１０２によりモンゴメリ型楕円曲線に変換可能と判断された標準型楕円曲線の曲線位数に関する情報を収集する（ステップ２０４）。与えられた楕円曲線の曲線位数に関する情報を収集することにより曲線位数を決定する曲線位数決定方法については R. Schoof, Elliptic curves over finite fields and the computation of square roots mod p, Math. Comp. 44 (1985), 483-494 に記載されている。コファクタ判定部１０６では曲線位数情報収集部１０７により取得した曲線位数の情報からコファクタが安全性の条件より与えられる値より小さいかどうかを判定し（ステップ２０５）、コファクタの値が大きければ、楕円曲線候補生成部１０４により標準型楕円曲線の再生成を行ない、上記手順に従ってモンゴメリ型楕円曲線に変換可能な標準型楕円曲線の曲線位数に関する情報から、再

度コファクタ判定部１０６によりコファクタの値が小さいかどうかの判定を行ない、コファクタの値が小さいと判定されるまで以上の手順を繰り返す。コファクタの値が小さければ、上記手順により生成されたモンゴメリ型楕円曲線に変換可能であり且つ安全な標準型楕円曲線を曲線パラメタとして出力を行なう（ステップ２０６）。

変換可能判定部１０２では以下の手順により標準型楕円曲線がモンゴメリ型楕円曲線に変換可能かを判定する。ここで、変換可能判定の一実施例を図３のフローチャートを用いて説明する。解の存在判定において標準型楕円曲線 $y^2 = f(x) = x^3 + ax + b$ に対して $f(\alpha) = 0$ となる $F_p$ の元 $\alpha$ が存在するかを調べる（ステップ３０１）。そのような元 $\alpha$ が存在しなければ変換不可能と出力し終了する（ステップ３０４）。上記 $\alpha$ が存在すれば、平方剰余判定により、$f(\alpha) = 0$ となる $\alpha$ に対して、$f'(\alpha)$ が $F_p$ において平方剰余となる $\alpha$ が存在するかを判定する（ステップ３０２）。そのような $\alpha$ が存在すれば変換可能と出力し終了する（ステップ３０３）。そのような $\alpha$ が存在しなければ変換不可能と出力して終了する（ステップ３０４）。ここで平方剰余とは素数 $p$ を法として平方根が存在する時をいい、存在しない場合は平方非剰余という。

以上の手順により変換可能の判定ができるということの根拠は以下の通りである。モンゴメリ型楕円曲線には $(0,0)$ という２倍すると無限遠点となる点があり、標準型楕円曲線には一般的にはそのような点があるとは限らないので、変換可能となるためには、標準型楕円曲線上の点で、２倍すると無限遠点になる点の存在が必要である。一般に $m$ 倍して初めて無限遠点となる点のことを位数 $m$ の点という。$f(\alpha) = 0$ となる $\alpha$ に対して、$(\alpha,0)$ は位数２の点である。変換可能とすれば、標準型楕円曲線上の位数２の点で、変換後に $(0,0)$ へ移る点が必要であり、$(\alpha,0)$ がそのような点とした場合に、標準型楕円曲線の点からモンゴメリ型楕円

曲線の点への変換は、ある $s,t \in F_p$ に対して $X = s(x-\alpha), Y = ty$ $(s \neq 0, t \neq 0)$ と表されなければならない。$(X,Y)$ はモンゴメリ型楕円曲線上の点であるので $BY^2 = X^3 + AX^2 + X$ をみたし、$X,Y$ にそれぞれ $s(x-\alpha), ty$ を代入すると、$Bt^2y^2 = s^3(x-\alpha)^3 + As^2(x-\alpha)^2 + s(x-\alpha)$ となる。$(x,y)$ は標準型楕円曲線上の点であるので、この式に $y^2 = f(x)$ を代入すると、$Bt^2 f(x) = s^3(x-\alpha)^3 + As^2(x-\alpha)^2 + s(x-\alpha)$ となる。$x^3$ の項を比較することにより、$Bt^2 = s^3$ を得る。これを上の式に代入すると、$s \neq 0$ であるから、$s^2 f(x) = s^2(x-\alpha)^3 + As(x-\alpha)^2 + (x-\alpha)$ となる。この式を $x$ で微分し、$x$ に $\alpha$ を代入すると、$s^2 f'(\alpha) = 1$ を得る。$s$ は $F_p$ の元であるから、$f'(\alpha)$ は平方剰余でなければならない。またその時、$A = 3\alpha s, B = s^3 / t^2$ である。逆に $f'(\alpha)$ が平方剰余であれば、$s = t = f'(\alpha)^{-1/2}, A = 3\alpha s, B = s$ とおけばモンゴメリ型楕円曲線 $BY^2 = X^3 + AX^2 + X$ に変換可能である。

以上により、変換可能であるためには、モンゴメリ型楕円曲線及び標準型楕円曲線上のそれぞれ位数２の点がお互いに移りあうことが必要であることを基にして、上記手順により変換可能の判定を行なえることが示された。

またモンゴメリ型楕円曲線の曲線位数は４で割れることが次のようにして分かる。モンゴメリ型楕円曲線上の点 $(0,0)$ は位数２の点である。$X^2 + AX + 1$ の判別式 $A^2 - 4$ が平方剰余であれば、$X^2 + AX + 1$ は $F_p$ において根を持ち、したがって $(0,0)$ 以外に位数２の点が２つ存在するので曲線位数は４で割れる。$A^2 - 4$ が平方非剰余であれば、$A+2$ 及び $A-2$ のうち一方のみが平方剰余であり他方は平方非剰余である。そのため $(A+2)/B$ 及び $(A-2)/B$ の一方が平方剰余となる。$(A+2)/B$ が平方剰余の場合はその平方根を $\gamma$ として $(1,\pm\gamma)$ が、$(A-2)/B$ が平方剰余の時はその平方根を $\gamma'$ として $(-1,\pm\gamma')$ がそれぞれ位数４の点となり、曲線位数は４で割れる。したがっていずれの場合においても曲線位数は４で割れる。

ここで、楕円曲線における演算速度は定義体の大きさに依存し、大きくなると遅くなる。楕円曲線の安全性は曲線位数に含まれる最大の素数の大きさに依存し、大きければ安全である。定義体の大きさを固定した時に、安全性を高くするためにはコファクタを小さくしなければならない。モンゴメリ型楕円曲線の曲線位数は４で割れるのでコファクタは４以上となり、定義体の大きさを固定してもっとも安全性を高めるにはコファクタは４にする必要がある。

尚、曲線位数を変換可能の判定条件に使わなければ、他の変換判定条件を用いることもできる。文献「楕円曲線暗号演算の計算方法について」１９９９年暗号と情報セキュリティシンポジウム予稿集 vol. 1, (1999) 275-280. の２７８ページにはそのような方法が記載されている。

次に、図１４の楕円暗号システムにおける曲線パラメタ生成サーバ１４０１内でのモンゴメリ型楕円曲線に変換可能であり且つ安全な標準型楕円曲線の生成方法の第１実施例の応用例を図１、図４を用いて説明する。図４は、楕円曲線パラメタ生成装置１０１における標準型楕円曲線の曲線パラメタの生成方法を示すフローチャートである。

楕円曲線パラメタ生成装置１０１では、定義体情報１０３を入力し、以下の手順により曲線パラメタ１０８を出力する。ここで定義体情報１０３は図２７における、定義体のビット長を含んだ定義体情報２７０１もしくは定義体素数を含んだ定義体情報２７０４で与えられている。楕円曲線候補生成部１０４において、定義体情報１０３よりランダムな標準型楕円曲線を生成する（ステップ４０１）。標準型楕円曲線 $y^2 = f(x) = x^3 + ax + b$ に対して、標準型楕円曲線 $y^2 = f_r(x) = x^3 + ar^2x + br^3$ を標準型楕円曲線 $y^2 = x^3 + ax + b$ のツイストという。ただし、$r$ は $F_p$ において平方非剰余な元である。ツイストに対し

て標準型楕円曲線$y^2 = x^3 + ax + b$を明示的にいう場合にはオリジナルという。変換可能判定部１０２において楕円曲線候補生成部１０４で生成された標準型楕円曲線及びそのツイストの標準型楕円曲線がモンゴメリ型楕円曲線に変換可能かの判定を行なうステップ（４０２）。オリジナルの標準型楕円曲線が変換可能であればツイストの標準型楕円曲線も変換可能である。共に変換不可能であれば楕円曲線候補生成部１０４で標準型楕円曲線の再生成を行ない、変換可能となるまで繰り返す。曲線位数情報収集部１０７では変換可能判定部１０２によりモンゴメリ型楕円曲線に変換可能と判断されたオリジナル及びツイストの標準型楕円曲線の曲線位数に関する情報を収集する（ステップ４０３）。コファクタ判定部１０６では曲線位数情報収集部１０７により取得したオリジナル及びツイストの曲線位数の情報からそれぞれのコファクタが安全性の条件から与えられる値より小さいかどうかを判定し（ステップ４０４）、共にコファクタが大きければ、楕円曲線候補生成部１０４により標準型楕円曲線の再生成を行ない、上記手順に従ってモンゴメリ型楕円曲線に変換可能な標準型楕円曲線の曲線位数に関する情報から、再度コファクタ判定部１０６によりそれぞれのコファクタが小さいかどうかの判定を行ない、いずれかのコファクタが小さいと判定されるまで以上の手順を繰り返す。いずれかのコファクタが小さければ、上記手順により生成されたモンゴメリ型楕円曲線に変換可能であり且つ安全な標準型楕円曲線を曲線パラメタとして出力を行なう（ステップ４０５）。以上の応用例では、オリジナル及びツイストの標準型楕円曲線のモンゴメリ型楕円曲線への変換可能性の判定を一度に行うため、安定性判定を行う標準型楕円曲線の候補を増やせることとなり、更に曲線生成が高速化される。

オリジナルの標準型楕円曲線がモンゴメリ型楕円曲線に変換可能である時、そのツイストの標準型楕円曲線もモンゴメリ型楕円曲線に変換

可能であることの根拠は以下の通りである。オリジナルの標準型楕円曲線がモンゴメリ型楕円曲線に変換可能であるので、$f(\alpha)=0$且つ$f'(\alpha)$が平方剰余であるαが存在する。その時$f_r(r\alpha)=0$であり、$f_r'(r\alpha)=r^2f'(\alpha)$であるので$f_r'(r\alpha)$は平方剰余である。従ってツイストの標準型楕円曲線もモンゴメリ型楕円曲線に変換可能である。また、オリジナルの標準型楕円曲線はツイストの標準型楕円曲線のツイストであるため、ツイストの標準型楕円曲線がモンゴメリ型楕円曲線に変換可能であればオリジナルの楕円曲線もモンゴメリ型楕円曲線に変換可能である。オリジナルの標準型楕円曲線$y^2=x^3+ax+b$がモンゴメリ型楕円曲線$BY^2=X^3+AX^2+X$に変換される時、ツイストの標準型楕円曲線$y^2=x^3+ar^2x+br^3$はモンゴメリ型楕円曲線$(B/r)Y^2=X^3+AX^2+X$に変換される。

図５は楕円暗号システムにおける曲線パラメタ生成サーバ内でのモンゴメリ型楕円曲線に変換可能であり且つその曲線位数が４×素数である、すなわちコファクタが４である標準型楕円曲線の生成方法の第２実施例を示す図である。図６は、第２実施例における楕円曲線パラメタ生成装置５０１におけるモンゴメリ型楕円曲線に変換可能且つコファクタが４である標準型楕円曲線の曲線パラメタの生成方法を示すフローチャートである。上述したとおり、モンゴメリ型楕円曲線に変換可能であるとすると、曲線位数が４の倍数になる。そのうち、安全性を高くするためには、曲線位数が４×素数が望ましい。

楕円曲線パラメタ生成装置５０１では定義体情報５０３を入力し、以下の手順により曲線パラメタ５０８を出力する。ここで定義体情報５０３は図２７における、定義体のビット長を含んだ定義体情報２７０１もしくは定義体素数を含んだ定義体情報２７０４で与えられている。標準型楕円曲線候補生成部５０４において、定義体情報５０３よりランダ

ムな標準型楕円曲線を生成する（ステップ６０１）。変換可能判定部５０２において楕円曲線候補生成部で生成された標準型楕円曲線がモンゴメリ型楕円曲線に変換可能かの判定を行なう（ステップ６０２）。変換不可能であれば標準型楕円曲線候補生成部５０４で標準型楕円曲線の再生成を行ない、変換可能となるまで繰り返す。８による整除性判定部５０５では変換可能判定部５０２によりモンゴメリ型楕円曲線に変換可能と判断された標準型楕円曲線の曲線位数が８で割れるかどうかを判定する（ステップ６０３）。上記楕円曲線の曲線位数が８で割れれば、楕円曲線候補生成部５０４により標準型楕円曲線の再生成を行ない、上記手順に従ってモンゴメリ型楕円曲線に変換可能な標準型楕円曲線の曲線位数が８で割れるかの判定を行ない、曲線位数が８で割れないと判定されるまで以上の手順を繰り返す。曲線位数が８で割れなければ、曲線位数情報収集部５０７により、モンゴメリ型楕円曲線に変換可能であり且つその曲線位数が８で割れない標準型楕円曲線の、曲線位数に関する情報を収集する（ステップ６０４）。コファクタ判定部５０６では曲線位数情報収集部５０７により取得した曲線位数の情報からコファクタが４であるかを判定し（ステップ６０５）、コファクタが４を越えると判定されれば、楕円曲線候補生成部５０４により標準型楕円曲線の再生成を行ない、上記手順に従ってモンゴメリ型楕円曲線に変換可能であり且つその曲線位数が８で割れない標準型楕円曲線の曲線位数に関する情報から、再度コファクタ判定部５０６によりコファクタが４であるかの判定を行ない、コファクタが４と判断されるまで以上の手順を繰り返す。コファクタが４であれば、上記手順により生成されたモンゴメリ型楕円曲線に変換可能であり且つそのコファクタが４である標準型楕円曲線を曲線パラメタとして出力を行なう（ステップ６０６）。

８による整除性判定部５０５は、以下の手順によりモンゴメリ型楕

円曲線に変換可能な標準型楕円曲線の曲線位数が８で割れるかどうかを判定する。図７及び図８は第２実施例における８による整除性判定方法を示すフローチャートである。

ステップ７０１により定義体素数が４を法として１であるか３であるかに応じて以下の処理を振り分ける。定義体素数の４を法とした値が１であればステップ７０２へ、３であればステップ８０１へ行く。ステップ７０２において、$f(x)=0$の$F_p$における根の数により処理を振り分ける。根の数が１個であればステップ７０４へ、３個であればステップ７０３へ行く。ステップ７０３において、$(A+2)/B$が$F_p$において平方剰余であるかを判定する。平方剰余であれば曲線位数は８で割れる（ステップ７０５）。平方非剰余であれば曲線位数は８で割れない（ステップ７０６）。ステップ７０４において$f'(\alpha)^{1/2}$が$F_p$において平方剰余であるかを判定する。平方非剰余であれば曲線位数は８で割れない（ステップ７０６）。平方剰余であれば曲線位数は８で割れる（ステップ７０５）。以上により、定義体素数の４を法とする値が１の時に対して曲線位数が８で割れるかを判定できる。定義体素数の４を法とする値が３の場合は、ステップ８０１において$f(x)=0$の$F_p$における根の数により処理を振り分ける。根の数が１個であればステップ８０２へ、３個であれば曲線位数は８で割れる（ステップ７０５）。ステップ８０２において、$A+2$が$F_p$において平方剰余であるかを判定する。平方非剰余であれば曲線位数は８で割れない（ステップ７０６）。平方剰余であれば曲線位数は８で割れる（ステップ７０５）。以上により、定義体素数の４を法とする値が３の時に対して曲線位数が８で割れるかを判定できる。

以上の手順により、モンゴメリ型楕円曲線に変換可能な標準型楕円曲線の曲線位数に対する８による整除性の判定ができるということの根

拠は以下の通りである。$BY^2 = X^3 + AX^2 + X$を標準型楕円曲線から変換されたモンゴメリ型楕円曲線とする。まず$f(x) = 0$の$F_p$における根の数を１個とする。この時標準型楕円曲線上の点で位数が２であるものは$(\alpha,0)$ただ一つである。モンゴメリ型楕円曲線上の位数２の点の$x$座標は$X^3 + AX^2 + X = 0$の$F_p$上での根であり、モンゴメリ型楕円曲線上の点$(0,0)$は標準型楕円曲線上の点$(\alpha,0)$と対応するので、$X^2 + AX + 1 = 0$は$F_p$において根を持たない。従ってその判別式$A^2 - 4$は$F_p$において平方非剰余である。$(A+2)/B$乃至$(A-2)/B$が平方剰余であれば、その平方根の１つをそれぞれ$\gamma,\gamma'$とすれば、$(1,\pm\gamma)$もしくは$(-1,\pm\gamma')$が位数４の点となる。$A^2 - 4$は平方非剰余であるので$(A+2)/B$及び$(A-2)/B$のいずれか一方は平方剰余でなければならない。従ってこの場合に必ず位数４の点が存在する。

モンゴメリ型楕円曲線上のある点$(u,v)$がこの曲線上の他の点$(w,z)$の２倍点となると仮定する。点$(w,z)$における接線の式は$Y = ((3w^2 + 2Aw + 1)/2Bz)(X - w) + z$である。接線は$(u,-v)$で曲線と交わるので$(X,Y)$に$(u,-v)$を代入し、両辺に$2Bz$を掛けて２乗すると$4Bv^2Bz^2 = ((3w^2 + 2Aw + 1)(u - w) + 2Bz^2)^2$となる。$(w,z)$及び$(u,-v)$は曲線上の点であるので$Bz^2 = w^3 + Aw^2 + w$及び$Bv^2 = u^3 + Au^2 + u$をみたす。これを上式に代入すると$4(u^3+Au^2+u)(w^3+Aw^2+w) = ((3w^2+2Aw+1)(u-w)+2(w^3+2Aw^2+w))^2$となる。点$(w,z)$で曲線と接線は接していて、また$w$と$u$は異なるので、$(u-w)^2$で割ることができ$(3w^2 + 2Aw + 1)^2 - 4(w^3 + Aw^2 + w)(u + A + 2w) = 0$となる。$w$の式とみて整理すると$w^4 - 4uw^3 - (4Au + 2)w^2 - 4uw + 1 = 0$となり、$w \neq 0$なので、$w^2$で割って$w + 1/w$の式とみて整理し直すと、$(w + 1/w)^2 - 4u(w + 1/w) - 4(Au + 1) = 0$となる。$w \in F_p$とすると$1/w \in F_p$であり、$w + 1/w \in F_p$となる。上の式が$w + 1/w$の方程式として$F_p$上で根を持つためには、その判別式$4(u^2 + Au + 1)$が平方剰余でなければならない。

$\varepsilon$ を $u^2+Au+1$ の平方根の一つとすると $w+1/w=2(u\pm\varepsilon)$ であり、この式が $w$ の方程式として $F_p$ 上で根を持つためには、判別式 $(u\pm\varepsilon)^2-1$ が平方剰余でなければならない。$((u+\varepsilon)^2-1)((u-\varepsilon)^2-1)=u^2(A^2-4)$ であり、$A^2-4$ は平方非剰余であるので、$(u+\varepsilon)^2-1$ 及び $(u-\varepsilon)^2-1$ のいずれか一方のみが平方剰余となる。その時 $w=(u\pm\varepsilon)\pm\sqrt{(u\pm\varepsilon)^2-1}$ であり、簡単のため $\delta=u\pm\varepsilon$ とおくと、$w^2+Aw+1=(2\delta+A)(\delta\pm\sqrt{\delta^2-1})$ なので $Bz^2=(2\delta+A)(\delta\pm\sqrt{\delta^2-1})^2$ となり、$z\in F_p$ であるためには $(2\delta+A)/B$ が平方剰余でなければならない。また、この場合も同様に $(2(u+\varepsilon)+A)(2(u-\varepsilon)+A)=A^2-4$ であるから、$(2(u+\varepsilon)+A)/B$ もしくは $(2(u-\varepsilon)+A)/B$ のいずれか一方のみが平方剰余となる。上記平方剰余に関する2つの二者択一条件において、共に同じ符号をとれば、$w,z\in F_p$ となる。$(u\pm\varepsilon)^2-1=u(2(u\pm\varepsilon)+A)$ と変形すると、$((u\pm\varepsilon)^2-1)((2(u\pm\varepsilon)+A)/B)=(u/B)(2(u\pm\varepsilon)+A)^2$ となる。したがって、$u/B$ が平方剰余であれば、上記平方剰余に関する2つの二者択一条件において共に同じ符号をとることができ、2倍すると点 $(u,v)$ となる点 $(w,z)$ が存在する。以上をまとめると $u^2+Au+1,u/B$ が共に平方剰余であれば、2倍すると点 $(u,v)$ となる点 $(w,z)$ が存在する、ということが示された。

位数4の点の $x$ 座標は $\pm1$ であり、したがって位数8の点の存在に関しては $A\pm2,B,-1$ の平方剰余性により表すことができる。

$-1$ が平方剰余であるのは定義体素数が4を法として1の時であり、$-1$ が平方非剰余であるのは定義体素数が4を法として3の時である。$f(x)=0$ の根の数が1個であるか3個であるかに応じて、$A^2-4$ が平方非剰余であるか平方剰余であるかが決まる。オリジナル及びツイストの曲線位数を加えると $2(p+1)$ であるので、$f(x)=0$ の根の数が3個の場合において、定義体素数が4を法として1の時は、オリジナルの曲線位数

が８で割れればツイストの曲線位数は８で割れず、オリジナルの曲線位数が８で割れなければツイストの曲線位数は８で割れる。また、定義体素数が４を法として３の時は、オリジナルの曲線位数が８で割れればツイストの曲線位数も８で割れ、オリジナルの曲線位数が８で割れなければツイストの曲線位数も８で割れない。以上をまとめると図９の通りである。図９により、図７及び図８のフローチャートの手順で判定を行なえば、曲線位数の８による整除性を判定できる。

上記８による整除性判定方法において、ステップ８０２の$A+2$の平方剰余判定は$A-2$の平方剰余判定を用いても行なうことができる。$f(x)=0$の根の数が１個の場合は$A^2-4$は平方非剰余なので、$A+2$が平方剰余であれば$A-2$は平方非剰余であり、$A+2$が平方非剰余であれば$A-2$は平方剰余であるので、$A-2$の平方剰余判定により判定可能である。ステップ７０３の$A+2$の平方剰余判定においても、$f(x)=0$の根の数が３個の場合は$A^2-4$は平方剰余なので、$(A+2)/B$が平方剰余であれば$(A-2)/B$も平方剰余であり、$(A+2)/B$が平方非剰余であれば$(A-2)/B$も平方非剰余であるので、$(A-2)/B$の平方剰余判定により判定可能である。ステップ７０４の$f'(\alpha)^{1/2}$の平方剰余判定においても、$f'(\alpha)^{1/2}$と$B$の平方剰余性は一致するので、$B$の平方剰余判定により判定可能である。

尚、第２実施例では、コファクタが４の場合を最適な実施例として、８による整除性判定方法を用いたが、本発明はこれに限定されるわけではなく、曲線位数＝コファクタ×素数の関係から導き出される他の整数であっても良い。

また、第２実施例においても、その応用例として図４を用いて説明した第１実施例の応用例と同様の方法が適用できる。

次に標準型楕円曲線の生成方法の第３実施例を説明する。

図１０は楕円暗号システムにおける曲線パラメタ生成サーバ内での

モンゴメリ型楕円曲線に変換可能であり且つその曲線位数が４×素数である、すなわちコファクタが４である標準型楕円曲線の生成方法の第３実施例を示す図である。図１１は、第３実施例における楕円曲線パラメタ生成装置１００１におけるモンゴメリ型楕円曲線に変換可能且つコファクタが４である標準型楕円曲線の曲線パラメタの生成方法を示すフローチャートである。

楕円曲線パラメタ生成装置１００１では定義体情報１００３を入力し、以下の手順により曲線パラメタ１００８を出力する。ここで定義体情報１００３は図２７における、定義体のビット長を含んだ定義体情報２７０１もしくは定義体素数を含んだ定義体情報２７０４で与えられている。楕円曲線候補生成部１００４において、定義体情報１００３よりランダムな標準型楕円曲線を生成する（ステップ１１０１）。適当性判定部１００２において楕円曲線候補生成部で生成された標準型楕円曲線及びそのツイストの標準型楕円曲線がモンゴメリ型楕円曲線に変換可能となり且つそれぞれの曲線位数が８で割れるかの判定を行なう（ステップ１１０２）。変換不可能であったり、変換可能であってもオリジナル及びツイストの標準型楕円曲線の曲線位数が共に８で割れれば標準型楕円曲線候補生成部１００４で標準型楕円曲線の再生成を行ない、モンゴメリ型楕円曲線に変換可能であり且つオリジナル及びツイストの標準型楕円曲線の曲線位数のいずれか一方が８で割れないと判断されるまで繰り返す。モンゴメリ型楕円曲線に変換可能であり且つオリジナル及びツイストの標準型楕円曲線のいずれか一方の曲線位数が８で割れなければ、曲線位数情報収集部１００７により、モンゴメリ型楕円曲線に変換可能であり且つその曲線位数もしくはツイストの曲線位数が８で割れない標準型楕円曲線の、曲線位数に関する情報を収集する（ステップ１１０３）。コファクタ判定部１００６では曲線位数情報収集部１００７によ

り取得した曲線位数の情報からコファクタが４であるかを判定し（ステップ１１０４）、コファクタが４を越えれば、楕円曲線候補生成部１００４により標準型楕円曲線の再生成を行ない、上記手順に従ってモンゴメリ型楕円曲線に変換可能であり且つその曲線位数が８で割れない標準型楕円曲線の曲線位数に関する情報から、再度コファクタ判定部１００６によりコファクタが４であるかの判定を行ない、コファクタが４と判断されるまで以上の手順を繰り返す。コファクタが４であれば、上記手順により生成されたモンゴメリ型楕円曲線に変換可能であり且つそのコファクタが４である標準型楕円曲線を曲線パラメタとして出力を行なう（ステップ１１０５）。

標準型楕円曲線に対する適当性判定部１００２は、与えられた標準型楕円曲線及びそのツイストの標準型楕円曲線が、モンゴメリ型楕円曲線に変換可能であり且つそれぞれの曲線位数が８で割れるかどうかを判定する。図１２及び図１３は第３実施例における標準型楕円曲線に対する適当性判定方法を示すフローチャートである。

ステップ１２０１により定義体素数が４を法として１であるか３であるかに応じて以下の処理を振り分ける。定義体素数の４を法とした値が１であればステップ１２０２へ、３であればステップ１３０１へ行く。ステップ１２０２において、$f(x)=0$の$F_p$における根の数により処理を振り分ける。根の数が１個であればステップ１２０４へ、３個であればステップ１２０３へ行く。$f(x)=0$が$F_p$において根を持たなければ、オリジナル及びツイストの標準型楕円曲線は共にモンゴメリ型楕円曲線に変換不可能であり不適当（１２０９）である。ステップ１２０３において、$f(\alpha)=0$となる$\alpha$のうち$f'(\alpha)$が$F_p$において平方剰余であるものを選択する。この$\alpha$に関して標準型楕円曲線はモンゴメリ型楕円曲線に変換可能である。ステップ１２０５において、$(A+2)/B$が$F_p$において平

方剰余であるかを判定する。平方剰余であればオリジナルの標準型楕円曲線の曲線位数は８で割れ、ツイストの標準型楕円曲線の曲線位数は８で割れないので、ツイストを選択する（ステップ１２０７）。平方非剰余であればツイストの標準型楕円曲線の曲線位数は８で割れ、オリジナルの標準型楕円曲線の曲線位数は８で割れないので、オリジナルを選択する（ステップ１２０８）。ステップ１２０４において、$f'(\alpha)$が$F_p$において平方剰余であるかを判定する。平方非剰余であれば、オリジナル及びツイストの標準型楕円曲線は共にモンゴメリ型楕円曲線に変換不可能であり不適当（１２０９）である。平方剰余であればステップ１２０６へ行く。この場合、標準型楕円曲線はモンゴメリ型楕円曲線に変換可能である。ステップ１２０６において$f'(\alpha)^{1/2}$が$F_p$において平方剰余であるかを判定する。平方非剰余であればツイストの標準型楕円曲線の曲線位数は８で割れ、オリジナルの標準型楕円曲線の曲線位数は８で割れないので、オリジナルを選択する（ステップ１２０８）。平方剰余であればオリジナルの標準型楕円曲線の曲線位数は８で割れ、ツイストの標準型楕円曲線の曲線位数は８で割れないので、ツイストを選択する（ステップ１２０７）。以上により、定義体素数の４を法とする値が１の時に対して、与えられたオリジナル及びツイストの標準型楕円曲線に対して、モンゴメリ型楕円曲線に変換可能であり且つ曲線位数が８で割れない標準型楕円曲線を選択する、あるいは不適当であるとして棄却するための判定を実行できる。定義体素数の４を法とする値が３の場合は、ステップ１３０１において$f(x)=0$の$F_p$における根の数により処理を振り分ける。根の数が１個であればステップ１３０２へ、３個もしくは$f(x)=0$が$F_p$において根を持たなければ、与えられたオリジナル及びツイストの標準型楕円曲線は共に変換不可能であったり変換可能であってもオリジナル及びツイストの曲線位数が共に８で割れるので不適当であ

る（ステップ１２０９）。ステップ１３０２において、$f'(\alpha)$が$F_p$において平方剰余であるかを判定する。平方非剰余であれば、オリジナル及びツイストの標準型楕円曲線は共に変換不可能であり不適当である（１２０９）。平方剰余であればステップ１３０３へ行く。この場合与えられたオリジナル及びツイストの標準型楕円曲線は共にモンゴメリ型楕円曲線に変換可能である。ステップ１３０３において、$A+2$が$F_p$において平方剰余であるかを判定する。平方非剰余であればオリジナル及びツイストの標準型楕円曲線の曲線位数は共に８で割れないので、オリジナル及びツイスト共に選択する（ステップ１３０５）。平方剰余であればオリジナル及びツイストの標準型楕円曲線の曲線位数は共に８で割れ、不適当である（ステップ１２０９）。以上により、定義体素数の４を法とする値が３の時に対して、与えられたオリジナル及びツイストの標準型楕円曲線に対して、モンゴメリ型楕円曲線に変換可能であり且つ曲線位数が８で割れない標準型楕円曲線を選択する、あるいは不適当であるとして棄却するための判定を実行できる。

以上の手順により、与えられたオリジナル及びツイストの標準型楕円曲線からモンゴメリ型楕円曲線に変換可能であり且つその曲線位数が８で割れない標準型楕円曲線を選択できる、あるいは不適当であるとして棄却できるということの根拠は以下の通りである。図１２及び図１３のフローチャートにおいて、前半は標準型楕円曲線がモンゴメリ型楕円曲線に変換可能であるかを判定しており、後半はモンゴメリ型楕円曲線に変換可能である標準型楕円曲線に対して、図９に基づき曲線位数が８で割れるかを判定している。オリジナルの標準型楕円曲線に対応するモンゴメリ型楕円曲線とツイストの標準型楕円曲線に対応するモンゴメリ型楕円曲線において、それぞれの$Y^2$の係数の平方剰余性は正反対になっていることに注意すればよい。ステップ１２０３において$f'(\alpha)$が

平方剰余となるαが必ず選択できる事については、Δを$f(x)$の判別式とすると$f(x)=0$の根が３個の場合にΔは平方剰余であり、他方$\alpha,\beta,\gamma$を$f(x)=0$の根とすると$\Delta=-16f'(\alpha)f'(\beta)f'(\gamma)$であるので、$f'(\alpha),f'(\beta),f'(\gamma)$のうち少なくとも１つは平方剰余である。

次に、図１４を用いて、モンゴメリ型楕円曲線に変換可能であり且つ安全な標準型楕円曲線の生成装置を組み込んだ楕円暗号システムを第４実施例として説明する。

曲線パラメタ生成サーバ１４０１は第１実施例におけるモンゴメリ型楕円曲線に変換可能であり且つ安全な標準型楕円曲線の生成を行なう楕円曲線パラメタ生成装置１０１を組み込んだサーバである。コンピュータＡ１４０２はモンゴメリ型楕円曲線を利用した楕円暗号により暗号化通信を行なうための秘密鍵公開鍵の組の生成を行なおうとしているコンピュータである。公開鍵サーバ１４０３は各コンピュータの公開鍵の登録を行ない、問い合わせがあれば問い合わせ対象のコンピュータの公開鍵を送信する。コンピュータＢ１４０４はコンピュータＡ１４０２へモンゴメリ型楕円曲線を利用して楕円暗号により暗号化通信を行なおうとしているコンピュータである。

第４実施例における楕円暗号システムでは以下の手順により楕円曲線パラメタ生成装置を利用して暗号化通信を行なう。図１５はそのフローチャートである。コンピュータＡ１４０２は曲線パラメタ生成サーバ１４０１にモンゴメリ型楕円曲線に変換可能であり且つ安全な標準型楕円曲線の生成を要請する（ステップ１５０１）。曲線パラメタ生成サーバ１４０１は上記曲線の生成要請に基づき、定義体情報１０３を楕円曲線パラメタ生成装置１０１に与えて曲線パラメタ１０８を生成する（ステップ１５０２）。ここで定義体情報１０３は図２７における、定義体のビット長を含んだ定義体情報２７０１もしくは定義体素数を含ん

だ定義体情報２７０４で与えられている。新規曲線パラメタとして、モンゴメリ型楕円曲線に変換可能な標準型楕円曲線の定義式及び曲線位数、標準型楕円曲線を変換したモンゴメリ型楕円曲線の定義式、及び標準型楕円曲線上の位数２の点でモンゴメリ型楕円曲線上の点$^{(0,0)}$に対応する点の$x$座標をコンピュータＡ１４０２に渡す（ステップ１５０３）。コンピュータＡ１４０２は与えられた新規曲線パラメタから秘密鍵公開鍵の組を作成する（ステップ１５０４）。コンピュータＡ１４０２は公開鍵サーバ１４０３に上記作成した公開鍵を登録する（ステップ１５０５）。コンピュータＢ１４０４は公開鍵サーバ１４０３にコンピュータＡ１４０２の公開鍵の問い合わせを行なう（ステップ１５０６）。公開鍵サーバ１４０３はコンピュータＢ１４０４の公開鍵問い合わせに基づき、コンピュータＡ１４０２の公開鍵をコンピュータＢ１４０４に渡す（１５０７）。コンピュータＢ１４０４はコンピュータＡ１４０２の公開鍵を用いてモンゴメリ型楕円曲線を利用して暗号化を行ない、コンピュータＡに暗号化通信を行なう（ステップ１５０８）。

図１６はモンゴメリ型楕円曲線に変換可能であり且つ安全な標準型楕円曲線の生成装置を組み込んだ楕円暗号システムの第５実施例を示す図である。

曲線パラメタ生成サーバ１６０１は第１実施例におけるモンゴメリ型楕円曲線に変換可能であり且つ安全な標準型楕円曲線の生成を行なう楕円曲線パラメタ生成装置１０１を組み込んだサーバである。コンピュータＡ１６０２はモンゴメリ型楕円曲線を利用した楕円暗号により暗号化通信を行なうための秘密鍵公開鍵の組の生成を行なおうとしているコンピュータである。公開鍵サーバ１６０３は各コンピュータの公開鍵の登録を行ない、問い合わせがあれば問い合わせ対象のコンピュータの公開鍵を送信する。コンピュータＢ１６０４はコンピュータＡ１６０

２へモンゴメリ型楕円曲線を利用して楕円暗号により暗号化通信を行なおうとしているコンピュータである。曲線パラメタ変換装置１６０５はモンゴメリ型楕円曲線に変換可能な標準型楕円曲線を与えるとその標準型楕円曲線に対応するモンゴメリ型楕円曲線及び標準型楕円曲線上の位数２の点でモンゴメリ型楕円曲線上の点$^{(0,0)}$に対応する点の$x$座標を出力するパラメタ変換装置である。

第５実施例における楕円暗号システムでは以下の手順により楕円曲線パラメタ生成装置を利用して暗号化通信を行なう。図１７はそのフローチャートである。コンピュータＡ１６０２は曲線パラメタ生成サーバ１６０１にモンゴメリ型楕円曲線に変換可能であり且つ安全な標準型楕円曲線の生成を要請する（ステップ１７０１）。曲線パラメタ生成サーバ１６０１は上記曲線の生成要請に基づき、定義体情報１０３を楕円曲線パラメタ生成装置１０１に与えて曲線パラメタ１０８を生成する（ステップ１７０２）。ここで定義体情報１０３は図２７における、定義体のビット長を含んだ定義体情報２７０１もしくは定義体素数を含んだ定義体情報２７０４で与えられている。新規曲線パラメタとして、モンゴメリ型楕円曲線に変換可能な標準型楕円曲線の定義式及び曲線位数をコンピュータＡ１６０２に渡す（ステップ１７０３）。コンピュータＡ１６０２は曲線パラメタ変換装置１６０５にモンゴメリ型楕円曲線に変換可能な標準型楕円曲線の定義式を与え、曲線パラメタ変換装置からモンゴメリ型楕円曲線に変換可能な標準型楕円曲線を変換したモンゴメリ型楕円曲線の定義式及び標準型楕円曲線上の位数２の点でモンゴメリ型楕円曲線上の点$^{(0,0)}$に対応する点の$x$座標を受け取る（ステップ１７０４）。コンピュータＡ１６０２は上記曲線パラメタから秘密鍵公開鍵の組を作成する（ステップ１７０５）。コンピュータＡ１６０２は公開鍵サーバ１６０３に上記作成した公開鍵を登録する（ステップ１７０

6）。コンピュータＢ１６０４は公開鍵サーバ１６０３にコンピュータＡ１６０２の公開鍵の問い合わせを行なう（ステップ１７０７）。公開鍵サーバ１６０３はコンピュータＢ１６０４の公開鍵問い合わせに基づき、コンピュータＡ１６０２の公開鍵をコンピュータＢ１６０４に渡す（ステップ１７０８）。コンピュータＢ１６０４はコンピュータＡ１６０２の公開鍵を用いてモンゴメリ型楕円曲線を利用して暗号化を行ない、コンピュータＡに暗号化通信を行なう（ステップ１７０９）。

図１８はモンゴメリ型楕円曲線に変換可能であり且つ安全な標準型楕円曲線の生成装置を組み込んだ楕円暗号システムの第６実施例を示す図である。

曲線パラメタ生成サーバ１８０１は第１実施例におけるモンゴメリ型楕円曲線に変換可能であり且つ安全な標準型楕円曲線の生成を行なう楕円曲線パラメタ生成装置１０１を組み込んだサーバである。コンピュータＡ１８０２はモンゴメリ型楕円曲線を利用した楕円暗号により暗号化通信を行なうための秘密鍵公開鍵の組の生成を行なおうとしているコンピュータである。公開鍵サーバ１８０３は各コンピュータの公開鍵の登録を行ない、問い合わせがあれば問い合わせ対象のコンピュータの公開鍵を送信する。コンピュータＢ１８０４はコンピュータＡ１８０２へモンゴメリ型楕円曲線を利用して楕円暗号により暗号化通信を行なおうとしているコンピュータである。曲線パラメタ変換装置１８０５はモンゴメリ型楕円曲線に変換可能な標準型楕円曲線を与えるとその標準型楕円曲線に対応するモンゴメリ型楕円曲線及び標準型楕円曲線上の位数２の点でモンゴメリ型楕円曲線上の点$^{(0,0)}$に対応する点の$x$座標を出力するパラメタ変換装置である。

第６実施例における楕円暗号システムでは以下の手順により楕円曲線パラメタ生成装置を利用して暗号化通信を行なう。図１９はそのフ

ローチャートである。コンピュータＡ１８０２は曲線パラメタ生成サーバ１８０１にモンゴメリ型楕円曲線に変換可能であり且つ安全な標準型楕円曲線の生成を要請する（ステップ１９０１）。曲線パラメタ生成サーバ１８０１は上記曲線の生成要請に基づき、定義体情報１０３を楕円曲線パラメタ生成装置１０１に与えて曲線パラメタ１０８を生成する（ステップ１９０２）。ここで定義体情報１０３は図２７における、定義体のビット長を含んだ定義体情報２７０１もしくは定義体素数を含んだ定義体情報２７０４で与えられている。新規曲線パラメタとして、モンゴメリ型楕円曲線に変換可能な標準型楕円曲線の定義式及び曲線位数をコンピュータＡ１８０２に渡す（ステップ１９０３）。コンピュータＡ１８０２は上記曲線パラメタから秘密鍵公開鍵の組を作成する（ステップ１９０４）。コンピュータＡは公開鍵サーバ１８０３に上記作成した公開鍵を登録する（ステップ１９０５）。公開鍵サーバ１８０３は曲線パラメタ変換装置１８０５にコンピュータＡ１８０２の公開鍵に関するモンゴメリ型楕円曲線に変換可能な標準型楕円曲線の定義式を与え、曲線パラメタ変換装置から上記モンゴメリ型楕円曲線に変換可能な標準型楕円曲線を変換したモンゴメリ型楕円曲線の定義式及び標準型楕円曲線上の位数２の点でモンゴメリ型楕円曲線上の点$^{(0,0)}$に対応する点の$x$座標を受け取り、コンピュータＡ１８０２の公開鍵の情報として加える（ステップ１９０６）。コンピュータＢ１８０４は公開鍵サーバ１８０３にコンピュータＡ１８０２の公開鍵の問い合わせを行なう（ステップ１９０７）。公開鍵サーバ１８０３はコンピュータＢ１８０４の公開鍵問い合わせに基づき、コンピュータＡ１８０２の公開鍵をコンピュータＢ１８０４に渡す（ステップ１９０８）。コンピュータＢ１８０４はコンピュータＡ１８０２の公開鍵を用いてモンゴメリ型楕円曲線を利用して暗号化を行ない、コンピュータＡ１８０２に暗号化通信を行なう（ス

テップ１９０９）。尚、ステップ１９０６とステップ１９０７は、その順番を問わず、コンピュータＢ１８０４が公開鍵サーバ１８０３にコンピュータＡ１８０２の公開鍵を問い合わせた後に、公開鍵サーバ１８０３が曲線パラメタ変換装置１８０５に標準型楕円曲線をモンゴメリ型楕円曲線に変換するよう要請しても良い。

図２０はモンゴメリ型楕円曲線に変換可能であり且つ安全な標準型楕円曲線の生成装置を組み込んだ楕円暗号システムの第７実施例を示す図である。

曲線パラメタ生成サーバ２００１は第１実施例におけるモンゴメリ型楕円曲線に変換可能であり且つ安全な標準型楕円曲線の生成を行なう楕円曲線パラメタ生成装置１０１を組み込んだサーバである。コンピュータＡ２００２はモンゴメリ型楕円曲線を利用した楕円暗号により暗号化通信を行なうための秘密鍵公開鍵の組の生成を行なおうとしているコンピュータである。公開鍵サーバ２００３は各コンピュータの公開鍵の登録を行ない、問い合わせがあれば問い合わせ対象のコンピュータの公開鍵を送信する。コンピュータＢ２００４はコンピュータＡ２００２へモンゴメリ型楕円曲線を利用して楕円暗号により暗号化通信を行なおうとしているコンピュータである。曲線パラメタ変換装置２００５はモンゴメリ型楕円曲線に変換可能な標準型楕円曲線を与えるとその標準型楕円曲線に対応するモンゴメリ型楕円曲線及び標準型楕円曲線上の位数２の点でモンゴメリ型楕円曲線上の点$^{(0,0)}$に対応する点の$x$座標を出力するパラメタ変換装置である。

第７実施例における楕円暗号システムでは以下の手順により楕円曲線パラメタ生成装置を利用して暗号化通信を行なう。図２１はそのフローチャートである。コンピュータＡ２００２は曲線パラメタ生成サーバ２００１にモンゴメリ型楕円曲線に変換可能であり且つ安全な標準型

楕円曲線の生成を要請する（ステップ２１０１）。曲線パラメタ生成サーバ２００１は上記曲線の生成要請に基づき、定義体情報１０３を楕円曲線パラメタ生成装置１０１に与えて曲線パラメタ１０８を生成する（ステップ２１０２）。ここで定義体情報１０３は図２７における、定義体のビット長を含んだ定義体情報２７０１もしくは定義体素数を含んだ定義体情報２７０４で与えられている。新規曲線パラメタとして、モンゴメリ型楕円曲線に変換可能な標準型楕円曲線の定義式及び曲線位数をコンピュータＡ２００２に渡す（ステップ２１０３）。コンピュータＡ２００２は上記曲線パラメタから秘密鍵公開鍵の組を作成する（ステップ２１０４）。コンピュータＡ２００２は公開鍵サーバ２００３に上記作成した公開鍵を登録する（ステップ２１０５）。コンピュータＢ２００４は公開鍵サーバ２００３にコンピュータＡ２００２の公開鍵の問い合わせを行なう（ステップ２１０６）。公開鍵サーバ２００３はコンピュータＢ２００４の公開鍵問い合わせに基づき、コンピュータＡ２００２の公開鍵をコンピュータＢ２００４に渡す（ステップ２１０７）。コンピュータＢは曲線パラメタ変換装置２００５にコンピュータＡ２００２の公開鍵に関するモンゴメリ型楕円曲線に変換可能な標準型楕円曲線の定義式を与え、曲線パラメタ変換装置から上記モンゴメリ型楕円曲線に変換可能な標準型楕円曲線を変換したモンゴメリ型楕円曲線の定義式及び標準型楕円曲線上の位数２の点でモンゴメリ型楕円曲線上の点$(0,0)$に対応する点の$x$座標を受け取り、コンピュータＡ２００２の公開鍵の情報として加える（ステップ２１０８）。コンピュータＢ２００４はコンピュータＡ２００２の公開鍵を用いてモンゴメリ型楕円曲線を利用して暗号化を行ない、コンピュータＡに暗号化通信を行なう（ステップ２１０９）。

図２２はモンゴメリ型楕円曲線に変換可能であり且つ安全な標準型

楕円曲線の生成装置における標準型楕円曲線からモンゴメリ型楕円曲線への変換可能判定を行なう変換可能判定装置の一実施例を示す図である。

変換可能判定装置２２０１は根存在判定部２２０２及び平方剰余判定部２２０３を用いて与えられた標準型楕円曲線がモンゴメリ型楕円曲線に変換可能であるかを判定する。根存在判定部２２０２では$f(x)=0$が$F_p$において根を持つか判定する。平方剰余判定部２２０３で$f'(\alpha)$が平方非剰余であると判定された根以外に根が存在しなければ変換不可能と出力する。根が存在すれば根を平方剰余判定部２２０３に与える。平方剰余判定部２２０３では$f(\alpha)=0$となる$\alpha$に対して、$f'(\alpha)$が$F_p$において平方剰余であるかを判定する。平方剰余であれば変換可能と出力する。平方非剰余であれば根存在判定部に他の根が存在するかを問い合わせる。

変換可能判定装置２２０１では以下の手順により、標準型楕円曲線がモンゴメリ型楕円曲線に変換可能かを判定する。図３のフローチャートを用いて説明する。ステップ３０１において標準型楕円曲線$y^2=f(x)=x^3+ax+b$に対して$f(\alpha)=0$となる$F_p$の元$\alpha$が存在するかを調べる。そのような元$\alpha$が存在しなければ変換不可能３０４と出力し終了する。上記$\alpha$が存在すれば、ステップ３０２により、$f(\alpha)=0$となる$\alpha$に対して、平方剰余判定部２２０３により$f'(\alpha)$が$F_p$において平方剰余かを判定し、その結果が平方剰余となる$\alpha$が存在するかを判定する。そのような$\alpha$が存在すれば変換可能３０３と出力し終了する。そのような$\alpha$が存在しなければ変換不可能３０４と出力して終了する。

図２３は図１６、図１８、図２０のモンゴメリ型楕円曲線に変換可能であり且つ安全な標準型楕円曲線の生成装置を組み込んだ楕円暗号システムにおける曲線パラメタ変換装置の一実施例を示す図である。

曲線パラメタ変換装置２３０１は根計算部２３０３、平方剰余判定部２３０２及び曲線パラメタ構成部２３０４を用いて、与えられたモン

ゴメリ型楕円曲線に変換可能な標準型楕円曲線から対応するモンゴメリ型楕円曲線及び点変換パラメタとして標準型楕円曲線上の位数２の点でモンゴメリ型楕円曲線上の点$(0,0)$に対応する点の$x$座標を計算し出力する。根計算部２３０３では$f(x)=0$の$F_p$における根$\alpha$を求める。平方剰余判定部２３０２では根計算部２３０３で求めた$\alpha$に対して、$f'(\alpha)$が$F_p$において平方剰余であるかを判定する。曲線パラメタ構成部２３０４では根計算部２３０３で求めた$\alpha$からモンゴメリ型楕円曲線を構成する。

曲線パラメタ変換装置２３０１では以下の手順により、モンゴメリ型楕円曲線に変換可能な標準型楕円曲線から変換されたモンゴメリ型楕円曲線及び標準型楕円曲線上の位数２の点でモンゴメリ型楕円曲線上の点$(0,0)$に対応する点の$x$座標を計算する。図２４のフローチャートを用いて説明する。ステップ２４０１により、$f(x)=0$の$F_p$における根$\alpha$を求める。ステップ２４０３において$f'(\alpha)$が$F_p$において平方剰余であるかを判定する。平方剰余であればステップ２４０４へ行く。平方非剰余であれば、ステップ２４０２により$f(x)=0$の根でステップ２４０３で$f'(\alpha)$が平方非剰余と分かった根$\alpha$以外の根を求める。その根を新たに$\alpha$とする。その$\alpha$に対して再度ステップ２４０３で$f'(\alpha)$が$F_p$において平方剰余であるかを判定する。$f(x)=0$の根は高々３個しかなく、またモンゴメリ型楕円曲線に変換可能であることが分かっているので、３回繰り返すうちに$f'(\alpha)$が平方剰余と判定されステップ２４０４へ進む。ステップ２４０４において、$s=f'(\alpha)^{-1/2}$を計算する。ステップ２４０５において、$B=s, A=3\alpha s$を計算する。ステップ２４０６において、$A, B, \alpha$を出力する。

このような曲線パラメタ変換装置により、図２７の標準型楕円曲線のみで与えられた曲線パラメタ２７０２を対応するモンゴメリ型楕円曲

線のデータを付け加えた曲線パラメタ２７０５に、標準型楕円曲線のみで与えられた公開鍵２７０３を対応するモンゴメリ型楕円曲線のデータを付け加えた公開鍵２７０６に変換できる。

図２５は$F_p$の拡大体$F_q$上定義された、モンゴメリ型楕円曲線に変換可能であり且つ安全な標準型楕円曲線の生成装置における標準型楕円曲線からモンゴメリ型楕円曲線への変換可能判定を行なう変換可能判定装置の一実施例を示す図である。

変換可能判定装置２５０１は根存在判定部２５０２及び平方根判定部２５０３を用いて、与えられた$F_q$上定義された標準型楕円曲線がモンゴメリ型楕円曲線に変換可能であるかを判定する。根存在判定部２５０２では$f(x)=0$が$F_q$において根を持つか判定する。平方根判定部２５０３で$f'(\alpha)$が平方非剰余であると判定された根以外に根が存在しなければ変換不可能と出力する。根が存在すれば根を平方根判定部２５０３に与える。平方根判定部２５０３では$f(\alpha)=0$となるαに対して、$f'(\alpha)$が$F_q$において平方根を持つかを判定する。平方根を持てば変換可能と出力する。平方根を持たなければ根存在判定部に$f(x)=0$の他の根が存在するかを問い合わせる。

変換可能判定装置２５０１では以下の手順により、$F_q$上定義された標準型楕円曲線がモンゴメリ型楕円曲線に変換可能かを判定する。図２６のフローチャートを用いて説明する。ステップ２６０１において標準型楕円曲線$y^2=f(x)=x^3+ax+b$に対して$f(\alpha)=0$となる$F_q$の元αが存在するかを調べる。そのような元αが存在しなければ変換不可能２６０４と出力し終了する。上記αが存在すれば、ステップ２６０２により、$f(\alpha)=0$となるαに対して、平方根判定部２５０３により$f'(\alpha)$が$F_q$において平方根を持つかを判定し、その結果が平方根を持つαが存在するかを判定する。そのようなαが存在すれば変換可能２６０３と出力し終

了する。そのようなαが存在しなければ変換不可能２６０４と出力して終了する。

図２８はモンゴメリ型楕円曲線に変換可能であり且つ安全な標準型楕円曲線の生成装置を組み込んだ楕円暗号システムにおいて公開鍵サーバ、コンピュータＡ乃至はコンピュータＢに組み込むための曲線置換管理装置の実施例を示す図である。

曲線置換管理装置２８０１は、判定曲線選択部２８０２、曲線置換判定部２８０３及び鍵テーブル２８０４を含む。鍵テーブル２８０４は曲線パラメタ及び公開鍵を含むデータテーブルである。

判定曲線選択部２８０２は指定時間もしくは一定時間毎に起動し、鍵テーブル２８０４より曲線パラメタを選択する。選択した曲線パラメタを曲線置換判定部２８０３に送る。曲線置換判定部２８０３は受け取った曲線パラメタに対して、曲線パラメタが作成された時間もしくはその曲線パラメタの利用者の数が、それぞれ安全性を保つために必要となる値よりも古いもしくは多い時に、与えられた曲線パラメタを新規の曲線パラメタに置換する必要があると出力する。

図２９は図２８の曲線置換管理装置を公開鍵サーバに組み込んだ場合における処理の流れを示すシーケンス図である。

曲線置換管理装置２９０３は曲線パラメタ置換要請を公開鍵サーバ２９０２に送る。公開鍵サーバ２９０２は曲線置換管理装置２９０３からの曲線パラメタ置換要請に基づき、曲線パラメタ生成要請を曲線パラメタ生成サーバ２９０１に送る。曲線パラメタ生成サーバ２９０１は公開鍵サーバ２９０２からの曲線パラメタ生成要請に基づき、新規曲線パラメタを生成し、新規曲線パラメタを公開鍵サーバ２９０２に送る。公開鍵サーバ２９０２は曲線パラメタを曲線パラメタ生成サーバ２９０１から受け取った新規曲線パラメタに置き換える。公開鍵サーバ２９０２

は、以前の曲線パラメタを利用しているコンピュータＡ２９０４に、新規曲線パラメタとともに新規公開鍵登録要請を送る。コンピュータＡ２９０４は、公開鍵サーバ２９０２からの新規公開鍵登録要請に基づき、受け取った新規曲線パラメタに対する秘密鍵公開鍵の組の生成を行なう。コンピュータＡ２９０４は生成した公開鍵を公開鍵サーバ２９０２に登録する。

以上述べたように本発明によれば、モンゴメリ型楕円曲線に変換可能であり且つ安全な標準型楕円曲線の生成において、安全な標準型楕円曲線の再生成を省くことができるので、上記性質を持った楕円曲線の生成にかかるコストを削減できる。暗号に利用する楕円曲線を定期的に上記性質を持つ新しい楕円曲線に置き換えることにより特定楕円曲線に対する攻撃を未然に防ぐ事ができ、さらにモンゴメリ型楕円曲線に変換可能であることからデータの暗号化復号化における時間を標準型楕円曲線を用いた場合よりも短縮することができる。

産業上の利用可能性

以上のとおり、本発明は、コンピュータネットワークにおけるセキュリティを行う上で有用であり、特に楕円暗号を用いたセキュリティ管理をおこなう環境に用いるのに適している。

# 請 求 の 範 囲

1．第１の楕円曲線を生成するステップと、前記第１の楕円曲線に関連する第２の楕円曲線を生成するステップと、前記第１の楕円曲線が第３の楕円曲線に変換可能であるかを判定するステップと、前記第１の楕円曲線が前記第３の楕円曲線に変換可能である場合、前記第１の楕円曲線及び前記第２の楕円曲線の安全性を判定するステップとを有することを特徴とする楕円曲線生成方法。

2．請求の範囲第１項記載の楕円曲線生成方法であって、前記第２の楕円曲線は前記第１の楕円曲線のツイストであることを特徴とする楕円曲線生成方法。

3．請求の範囲第１項記載の楕円曲線生成方法であって、前記第１の楕円曲線は$y^2=x^3+ax+b$であり、前記第２の楕円曲線は$y^2=x^3+ar^2x+br^3$であり、前記第３の楕円曲線は$BY^2=X^3+AX^2+X$であることを特徴とする楕円曲線生成方法。

4．請求の範囲第３項記載の楕円曲線生成方法であって、前記第３の楕円曲線に変換可能であるかを判定するステップは、前記第１の楕円曲線$y^2=f(x)$に対して、$f(\alpha)=0$となる$\alpha$が存在するかを判定するステップと、$f(\alpha)=0$となる$\alpha$に対して$f'(\alpha)$が平方根を持つかを判定するステップとからなることを特徴とする楕円曲線生成方法。

5．請求の範囲第１項記載の楕円曲線生成方法であって、前記第１の楕円曲線の安全性を判定するステップは、前記第１の楕円曲線の曲線位数に関する情報を抽出するステップと、前記曲線位数に関する情報からコファクタの判定を行うステップとを有することを特徴とする楕円曲線生成方法。

6．請求の範囲第１項記載の楕円曲線生成方法であって、予め定められ

た素数位数の体上定義された第１の楕円曲線を用いることを特徴とする楕円曲線生成方法。

７．第１の楕円曲線を生成するステップと、前記第１の楕円曲線が第２の楕円曲線に変換可能であるかを判定するステップと、前記第１の楕円曲線が前記第２の楕円曲線に変換可能である場合、前記第１の楕円曲線の安全性を判定するステップと、前記第1の楕円曲線が安全でないと判定された場合、前記第１の楕円曲線に付随する第３の楕円曲線の安全性を判定するステップとを有することを特徴とする楕円曲線生成方法。

８．楕円暗号における楕円曲線の生成方法であって、ランダムな標準型楕円曲線$y^2=x^3+ax+b$を生成するステップと、前記生成された標準型楕円曲線$y^2=x^3+ax+b$がモンゴメリ型楕円曲線$BY^2=X^3+AX^2+X$に変換可能であるかを判定するステップと、前記楕円曲線の曲線位数の８による整除性を判定するステップと、前記楕円曲線の曲線位数に関する情報を収集するステップと、前記曲線位数の情報からコファクタの値を判定するステップとからなり、モンゴメリ型楕円曲線に変換可能であり且つコファクタが４である標準型楕円曲線を生成することを特徴とする楕円曲線生成方法。

９．第１の楕円曲線$y^2=x^3+ax+b$を生成する楕円曲線候補生成部と、前記第１の楕円曲線が第２の楕円曲線$BY^2=X^3+AX^2+X$に変換可能であるかを判定する変換可能判定部と、前記第２の楕円曲線に変換可能な第１の楕円曲線の安全性を判定する安全性判定部とを備えたことを特徴とする楕円曲線生成装置。

１０．請求の範囲第９項記載の楕円曲線生成装置であって、前記変換可能判定部は、前記第１の楕円曲線に対して、$f(\alpha)=0$となる$\alpha$が存在するかを判定する根存在判定部と、$f(\alpha)=0$となる$\alpha$に対して$f'(\alpha)$が平方根を持つかを判定する平方根判定部とからなることを

特徴とする楕円曲線生成装置。

１１．請求の範囲第９項記載の楕円曲線生成装置であって、前記変換可能判定部は、前記第１の楕円曲線に対して、ｆ（α）＝０となるαが存在するかを判定する根存在判定部と、ｆ（α）＝０となるαに対してｆ’（α）が平方剰余であるかを判定する平方剰余判定部とからなることを特徴とする楕円曲線生成装置。

１２．第１の計算機と第２の計算機との間で暗号化通信を行う暗号システムで使用される楕円曲線生成装置であって、前記計算機から楕円曲線の生成要請を受け、モンゴメリ型楕円曲線に変換可能な標準型楕円曲線を生成することを特徴とする楕円曲線生成装置。

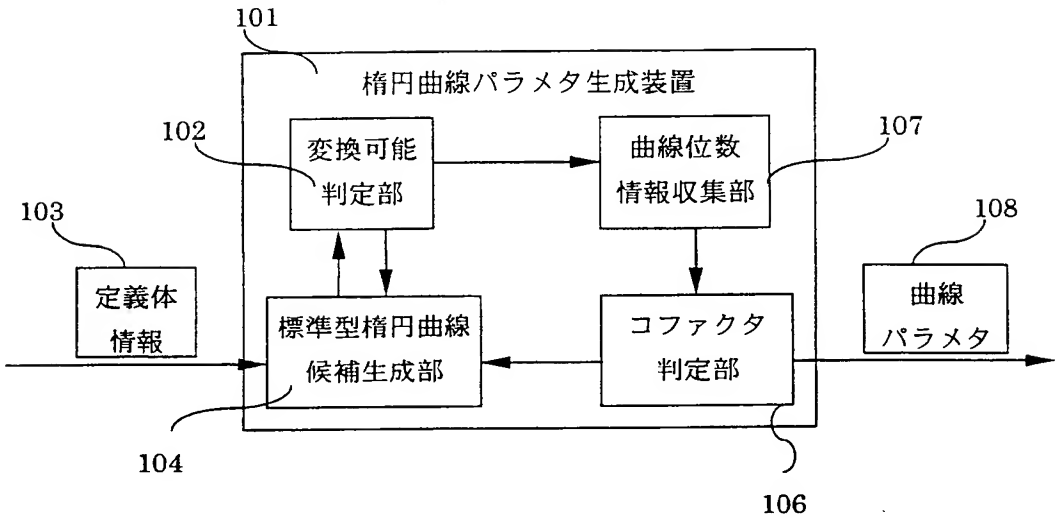
１３．楕円曲線生成方法を実行するプログラムを格納した記録媒体であって、前記楕円曲線生成方法は以下を含む：第１の楕円曲線$y^2=x^3+ax+b$を生成するステップと、前記第１の楕円曲線に関連する第２の楕円曲線$y^2=x^3+ar^2x+br^3$を生成するステップと、前記第１の楕円曲線が第３の楕円曲線$BY^2=X^3+AX^2+X$に変換可能であるかを判定するステップと、前記第３の楕円曲線に変換可能な第１の楕円曲線の安全性を判定するステップと、前記第２の楕円曲線の安全性を判定するステップ。

１４．楕円暗号を利用して暗号化通信を行う暗号システムであって、暗号化通信を受信する第１の計算機と、暗号化通信を送信する第２の計算機と、前記第１の計算機から楕円曲線の生成要請を受けて、モンゴメリ型楕円曲線に変換可能な標準型楕円曲線を生成する楕円曲線生成装置とを備えたことを特徴とする暗号システム。

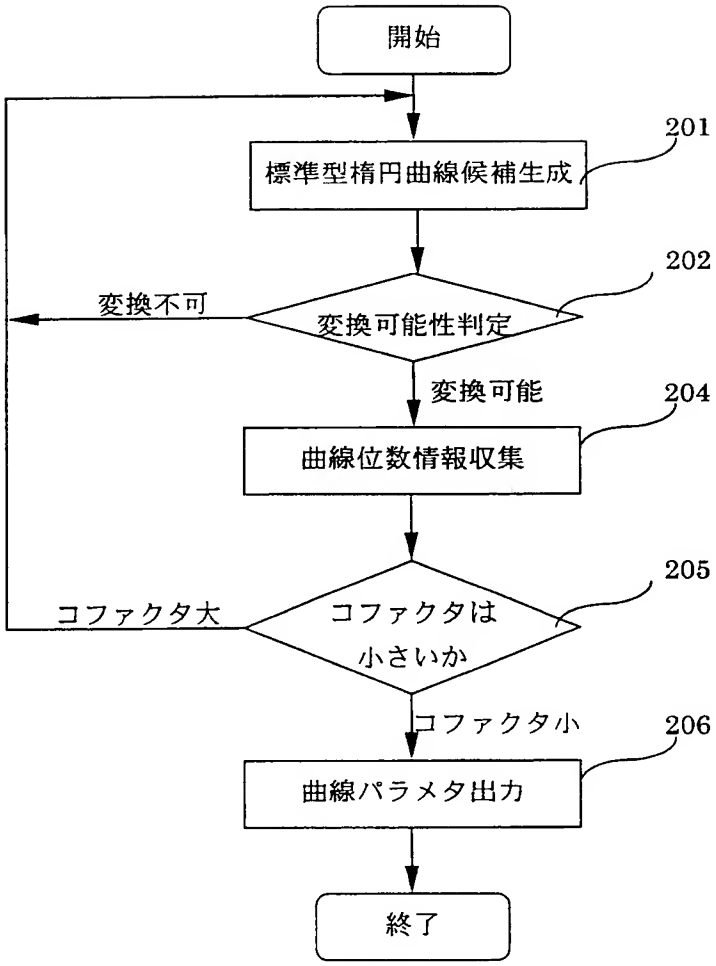
１５．請求の範囲第１４項記載の暗号システムであって、暗号化通信に使用している楕円曲線に置換の必要性があるか否かを管理する曲線置換管理装置を更に備え、前記楕円曲線に置換の必要性が生じた場合は、前

記楕円曲線生成装置が新たに生成した楕円曲線に置換して暗号化通信を行うことを特徴とする暗号システム。

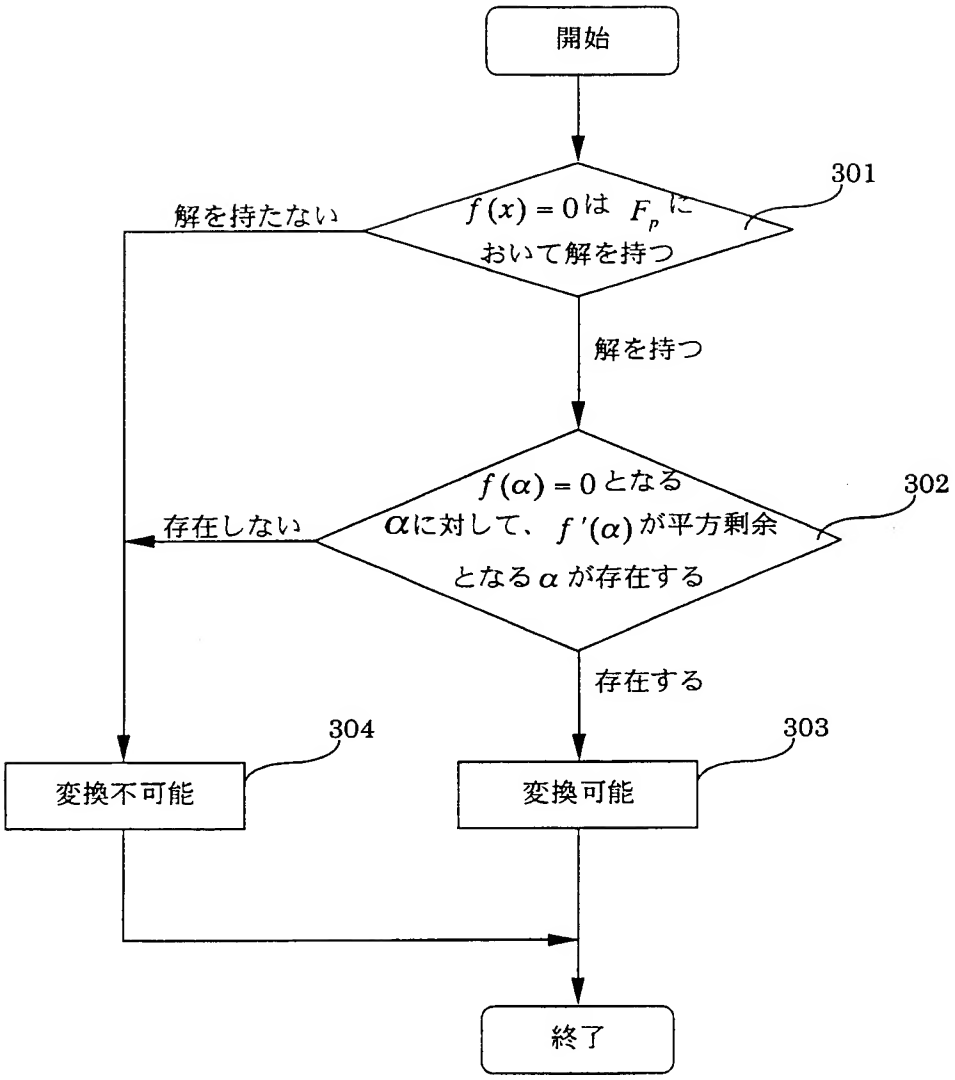
第 1 図


101
楕円曲線パラメタ生成装置
102
変換可能
判定部
107
曲線位数
情報収集部
103
定義体
情報
108
曲線
パラメタ
標準型楕円曲線
候補生成部
コファクタ
判定部
104
106

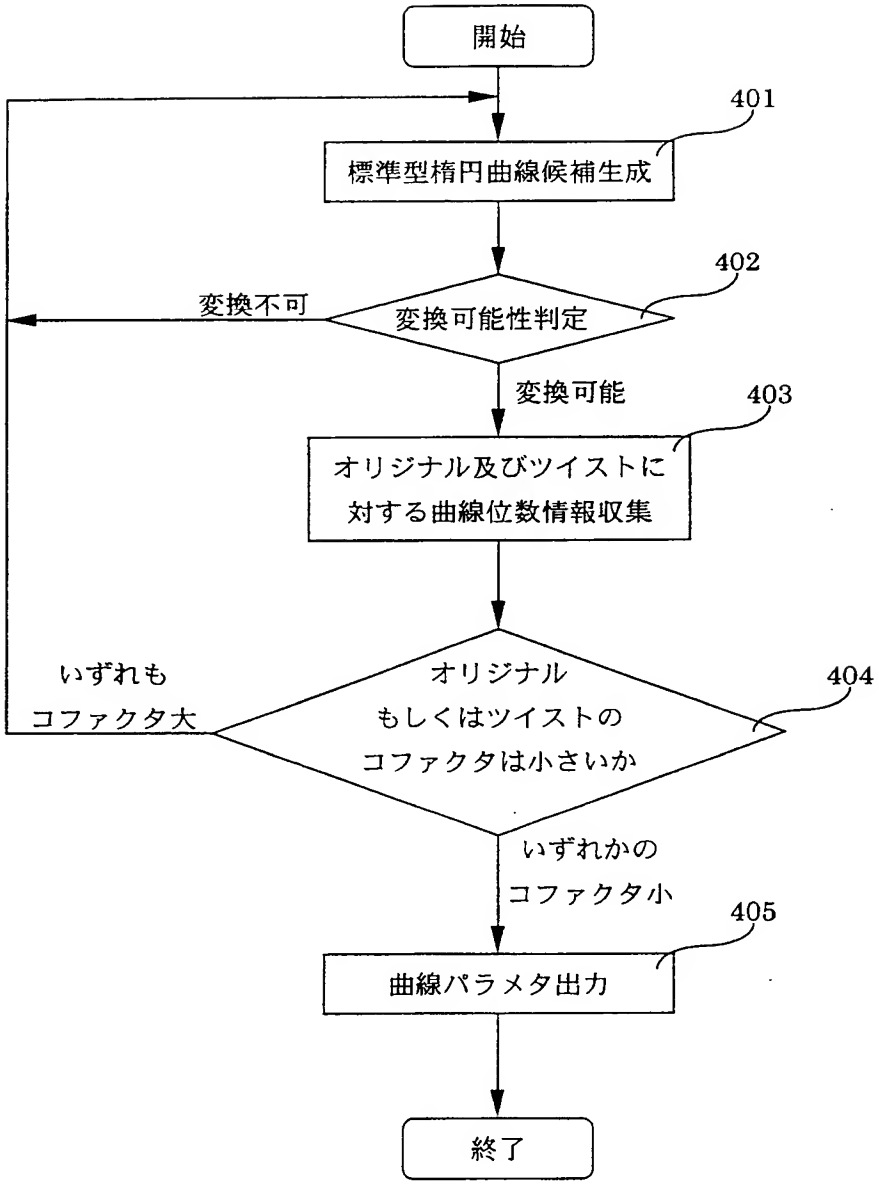
第２図


開始
201
標準型楕円曲線候補生成
202
変換不可
変換可能性判定
変換可能
204
曲線位数情報収集
205
コファクタ大
コファクタは
小さいか
コファクタ小
206
曲線パラメタ出力
終了

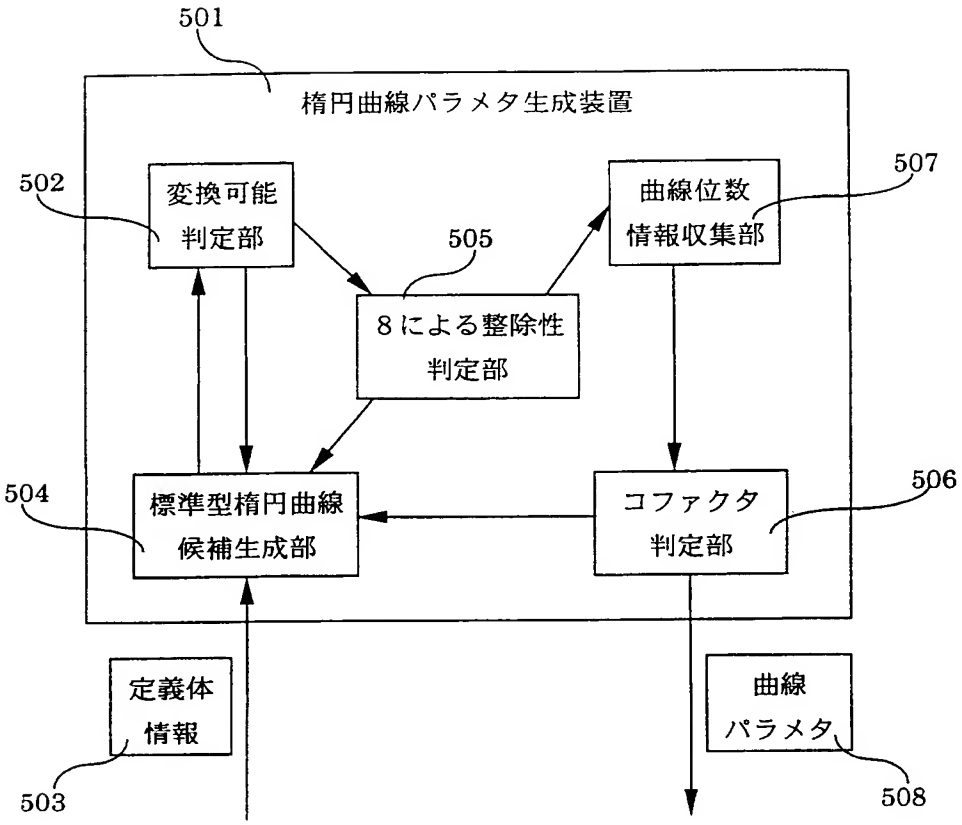
第３図


開始
$f(x)=0$は $F_p$ において解を持つ
301
解を持たない
解を持つ
$f(\alpha)=0$となる $\alpha$に対して、$f'(\alpha)$が平方剰余となる$\alpha$が存在する
302
存在しない
存在する
304
変換不可能
303
変換可能
終了

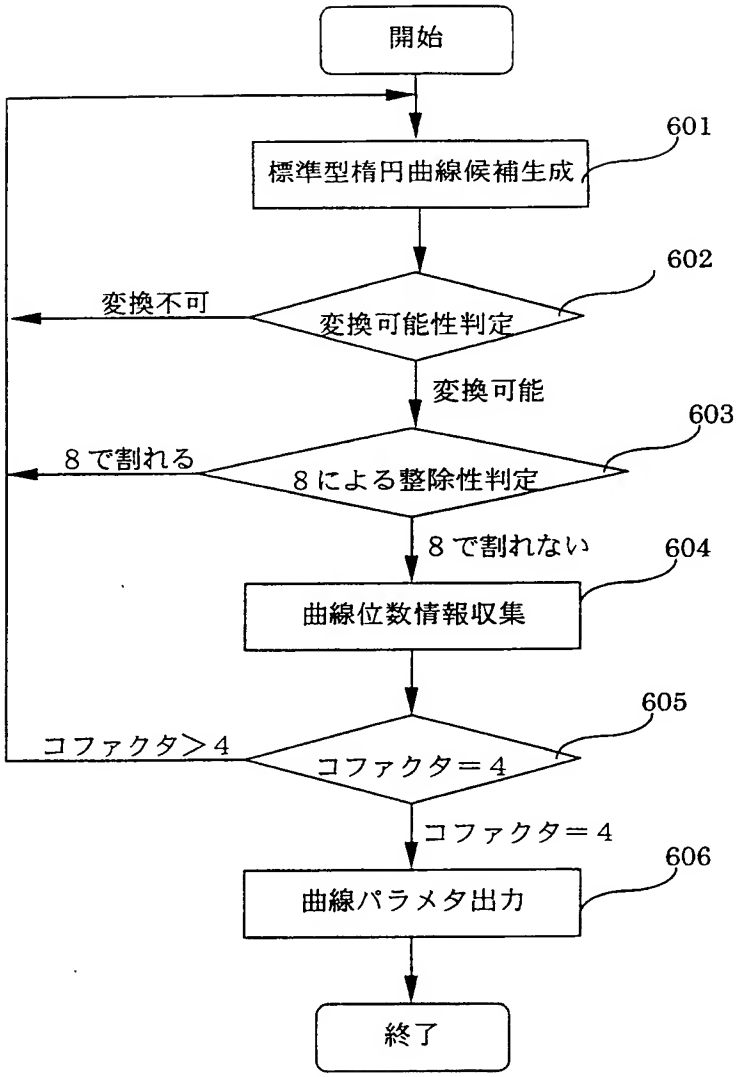
第 4 図


開始
401
標準型楕円曲線候補生成
402
変換不可
変換可能性判定
変換可能
403
オリジナル及びツイストに
対する曲線位数情報収集
いずれも
コファクタ大
オリジナル
もしくはツイストの
コファクタは小さいか
404
いずれかの
コファクタ小
405
曲線パラメタ出力
終了

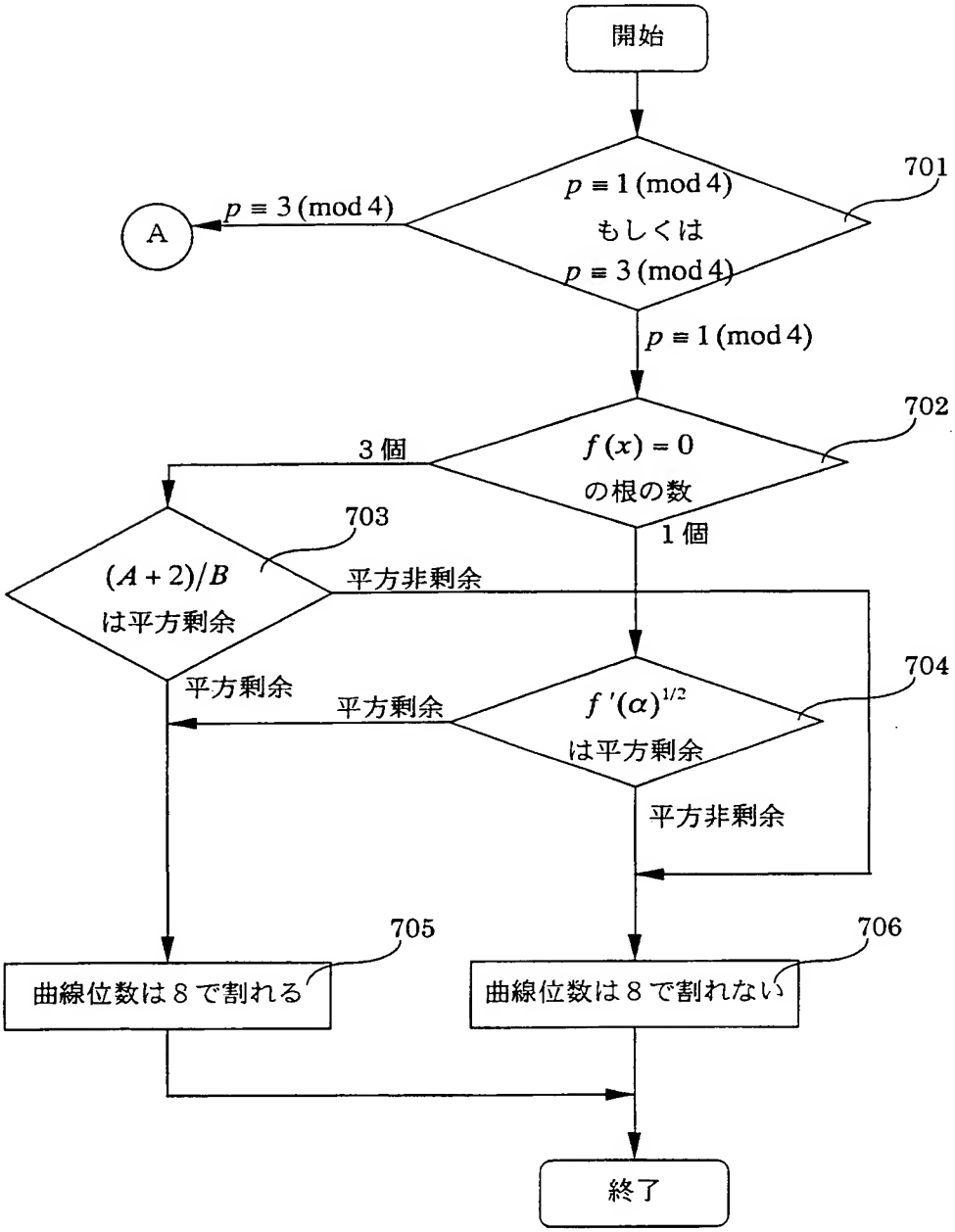
第５図


501
楕円曲線パラメタ生成装置
502
変換可能
判定部
505
８による整除性
判定部
507
曲線位数
情報収集部
504
標準型楕円曲線
候補生成部
506
コファクタ
判定部
定義体
情報
503
曲線
パラメタ
508

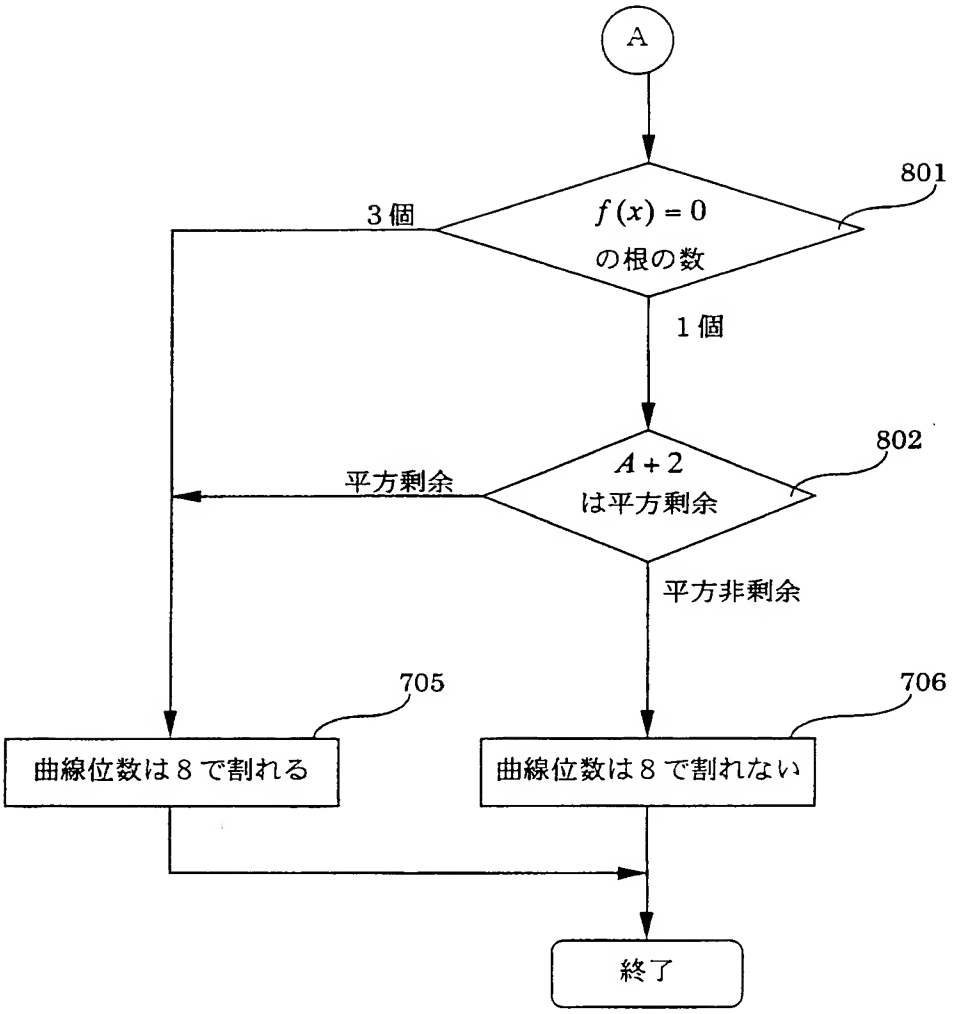
第６図


開始
601
標準型楕円曲線候補生成
602
変換不可
変換可能性判定
変換可能
603
８で割れる
８による整除性判定
８で割れない
604
曲線位数情報収集
605
コファクタ＞４
コファクタ＝４
コファクタ＝４
606
曲線パラメタ出力
終了

第7図


開始
701
$p \equiv 1 \pmod 4$
もしくは
$p \equiv 3 \pmod 4$
$p \equiv 3 \pmod 4$
A
$p \equiv 1 \pmod 4$
702
$f(x) = 0$
の根の数
3個
1個
703
$(A+2)/B$
は平方剰余
平方非剰余
平方剰余
平方剰余
704
$f'(\alpha)^{1/2}$
は平方剰余
平方非剰余
705
曲線位数は8で割れる
706
曲線位数は8で割れない
終了

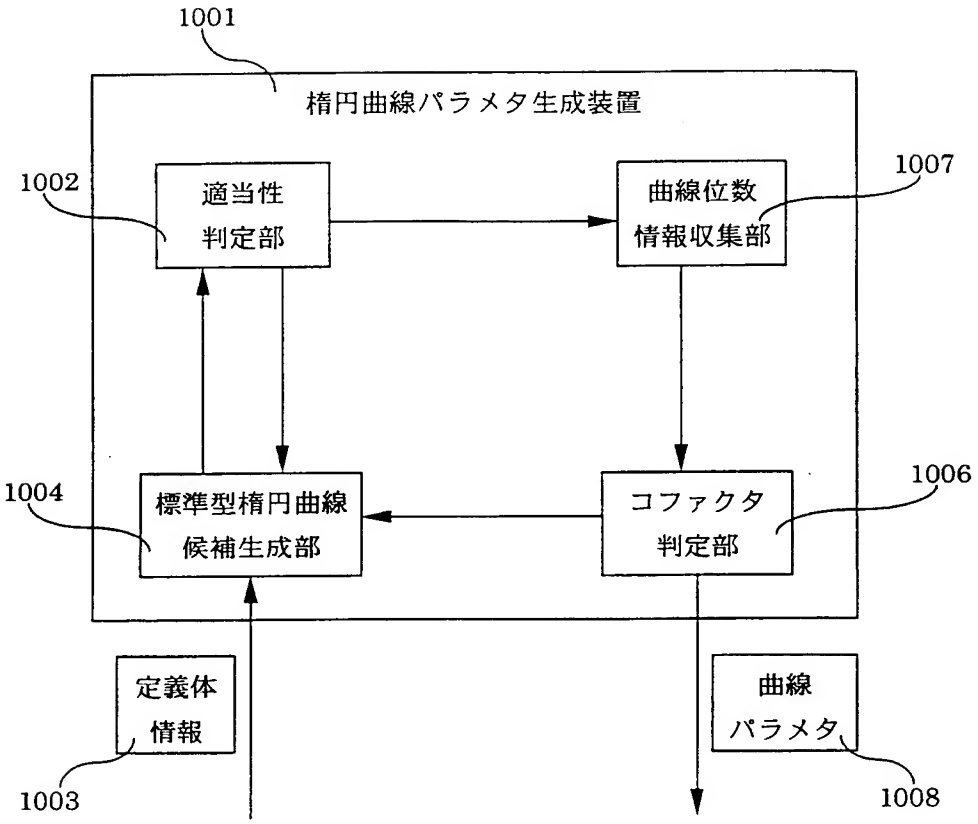
第８図


A
801
$f(x) = 0$
の根の数
3個
1個
802
$A + 2$
は平方剰余
平方剰余
平方非剰余
705
706
曲線位数は８で割れる
曲線位数は８で割れない
終了

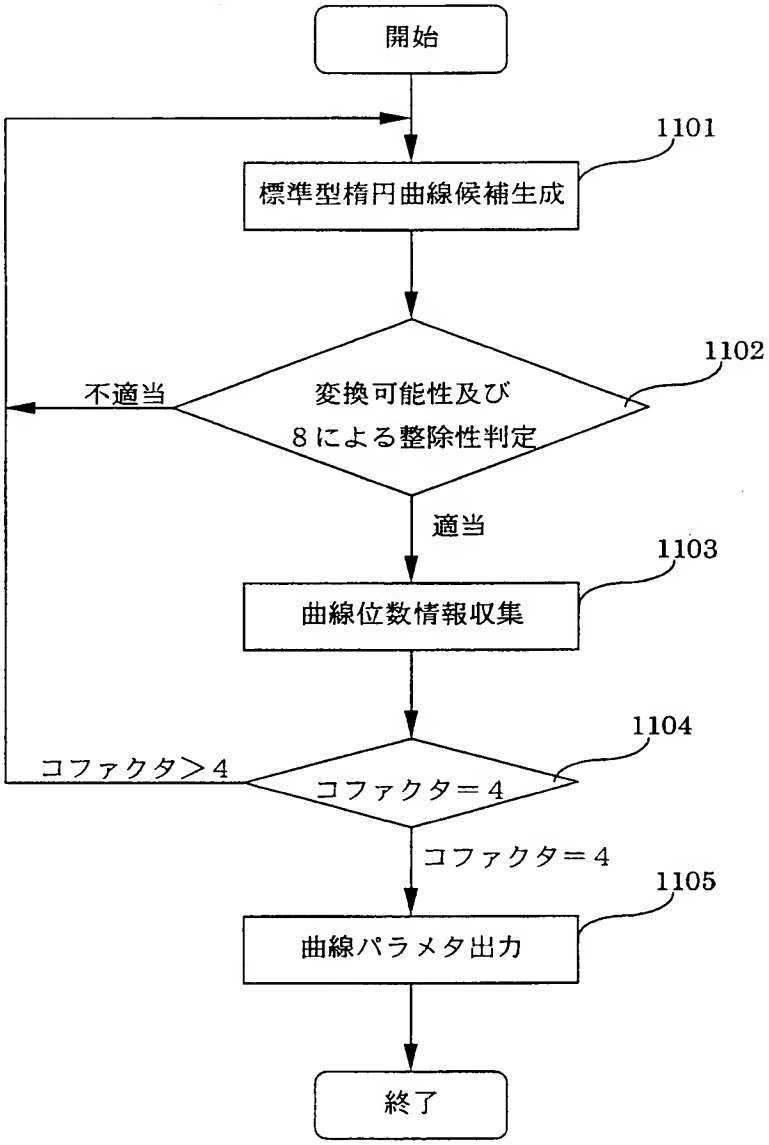
第９図

| －１ | Ａ＋２ | Ａ－２ | Ｂ | 曲線位数 |
|---|---|---|---|---|
| 平方剰余 | 平方剰余 | 平方非剰余 | 平方剰余 | ８で割れる |
| 平方剰余 | 平方剰余 | 平方非剰余 | 平方非剰余 | ８で割れない |
| 平方剰余 | 平方非剰余 | 平方剰余 | 平方剰余 | ８で割れる |
| 平方剰余 | 平方非剰余 | 平方剰余 | 平方非剰余 | ８で割れない |
| 平方剰余 | 平方剰余 | 平方剰余 | 平方剰余 | ８で割れる |
| 平方剰余 | 平方剰余 | 平方剰余 | 平方非剰余 | ８で割れない |
| 平方剰余 | 平方非剰余 | 平方非剰余 | 平方剰余 | ８で割れない |
| 平方剰余 | 平方非剰余 | 平方非剰余 | 平方非剰余 | ８で割れる |
| 平方非剰余 | 平方剰余 | 平方非剰余 | 平方剰余 | ８で割れる |
| 平方非剰余 | 平方剰余 | 平方非剰余 | 平方非剰余 | ８で割れる |
| 平方非剰余 | 平方非剰余 | 平方剰余 | 平方剰余 | ８で割れない |
| 平方非剰余 | 平方非剰余 | 平方剰余 | 平方非剰余 | ８で割れない |
| 平方非剰余 | 平方剰余 | 平方剰余 | 平方剰余 | ８で割れる |
| 平方非剰余 | 平方剰余 | 平方剰余 | 平方非剰余 | ８で割れる |
| 平方非剰余 | 平方非剰余 | 平方非剰余 | 平方剰余 | ８で割れる |
| 平方非剰余 | 平方非剰余 | 平方非剰余 | 平方非剰余 | ８で割れる |

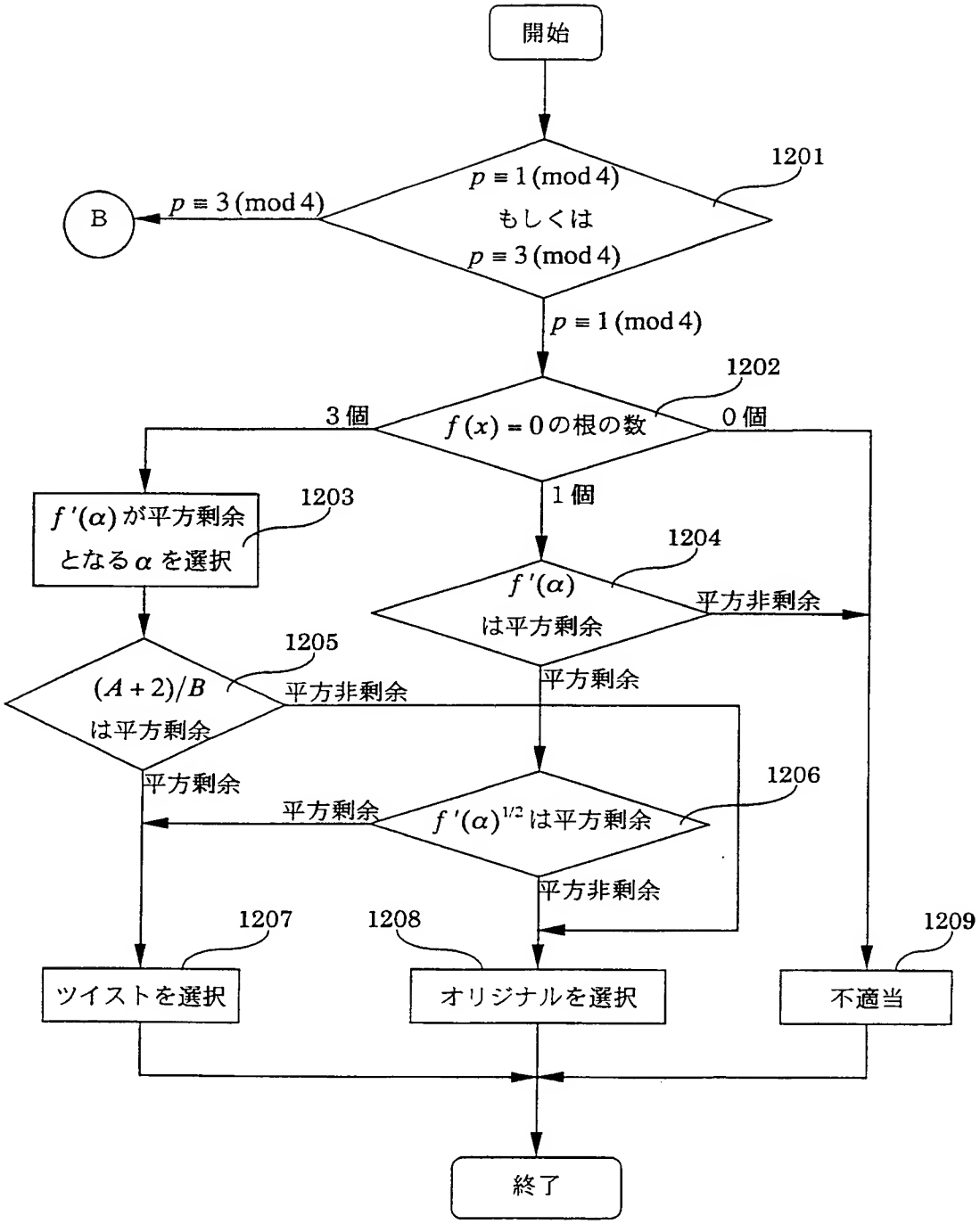
第 10 図


1001
楕円曲線パラメタ生成装置
1002
適当性
判定部
1007
曲線位数
情報収集部
1004
標準型楕円曲線
候補生成部
1006
コファクタ
判定部
定義体
情報
1003
曲線
パラメタ
1008

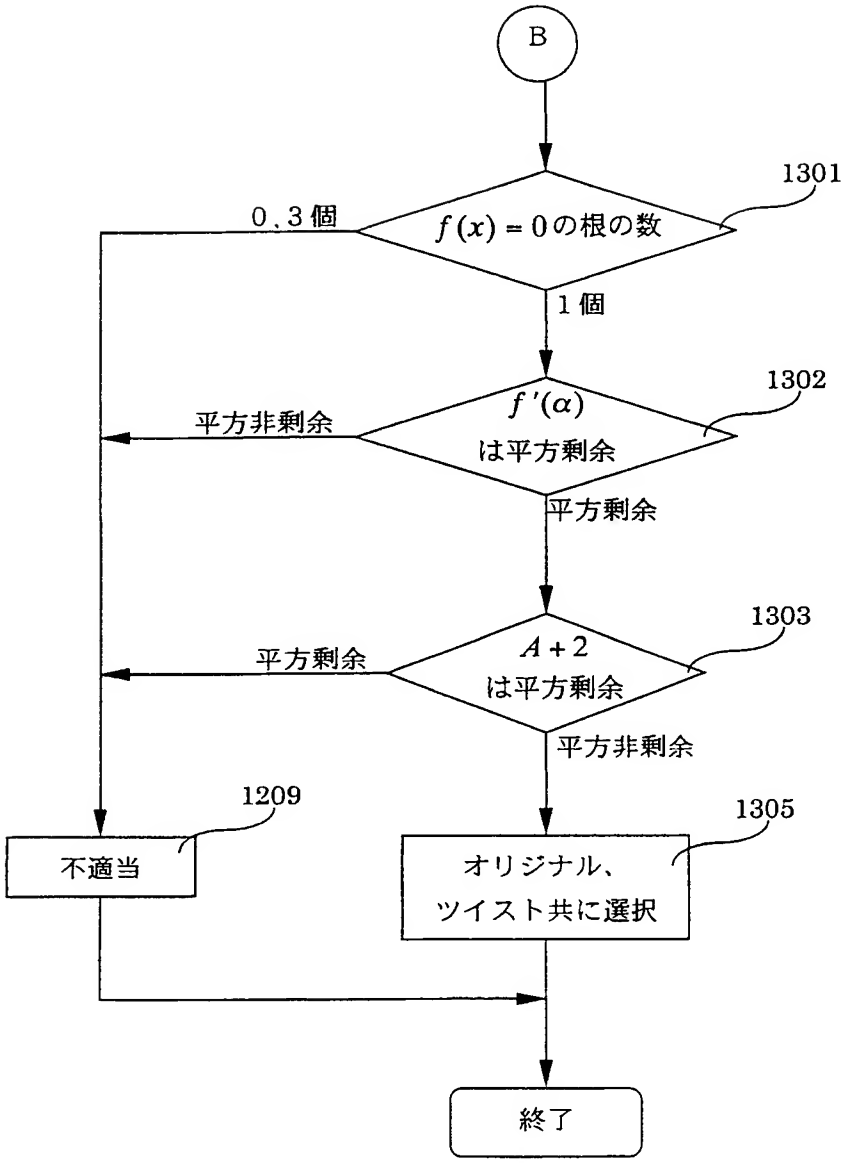
第 11 図


開始
1101
標準型楕円曲線候補生成
1102
変換可能性及び
8による整除性判定
不適当
適当
1103
曲線位数情報収集
1104
コファクタ＞4
コファクタ＝4
コファクタ＝4
1105
曲線パラメタ出力
終了

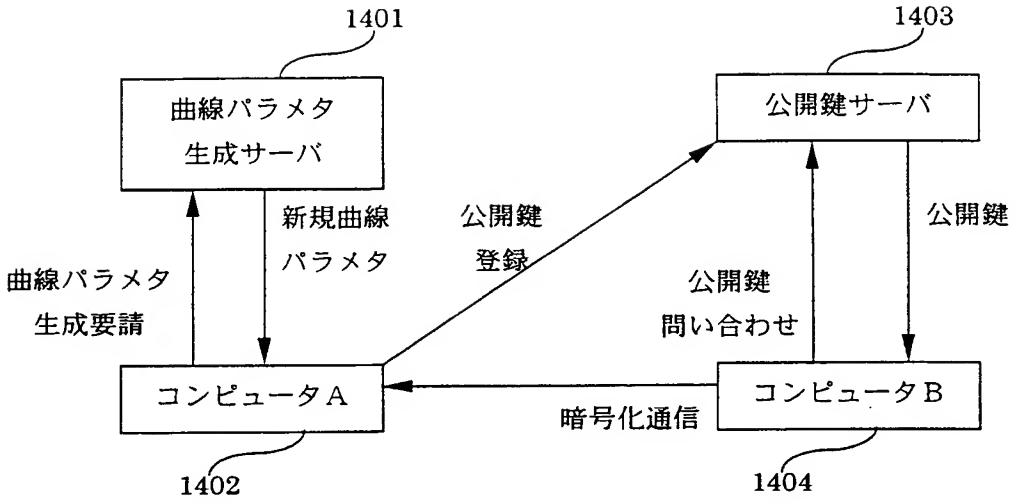
第 12 図


開始
1201
$p \equiv 1 \pmod 4$
もしくは
$p \equiv 3 \pmod 4$
B
$p \equiv 3 \pmod 4$
$p \equiv 1 \pmod 4$
1202
$f(x) = 0$の根の数
3個
0個
1個
1203
$f'(\alpha)$が平方剰余
となる$\alpha$を選択
1204
$f'(\alpha)$
は平方剰余
平方非剰余
平方剰余
1205
$(A+2)/B$
は平方剰余
平方非剰余
平方剰余
1206
$f'(\alpha)^{1/2}$は平方剰余
平方剰余
平方非剰余
1207
ツイストを選択
1208
オリジナルを選択
1209
不適当
終了

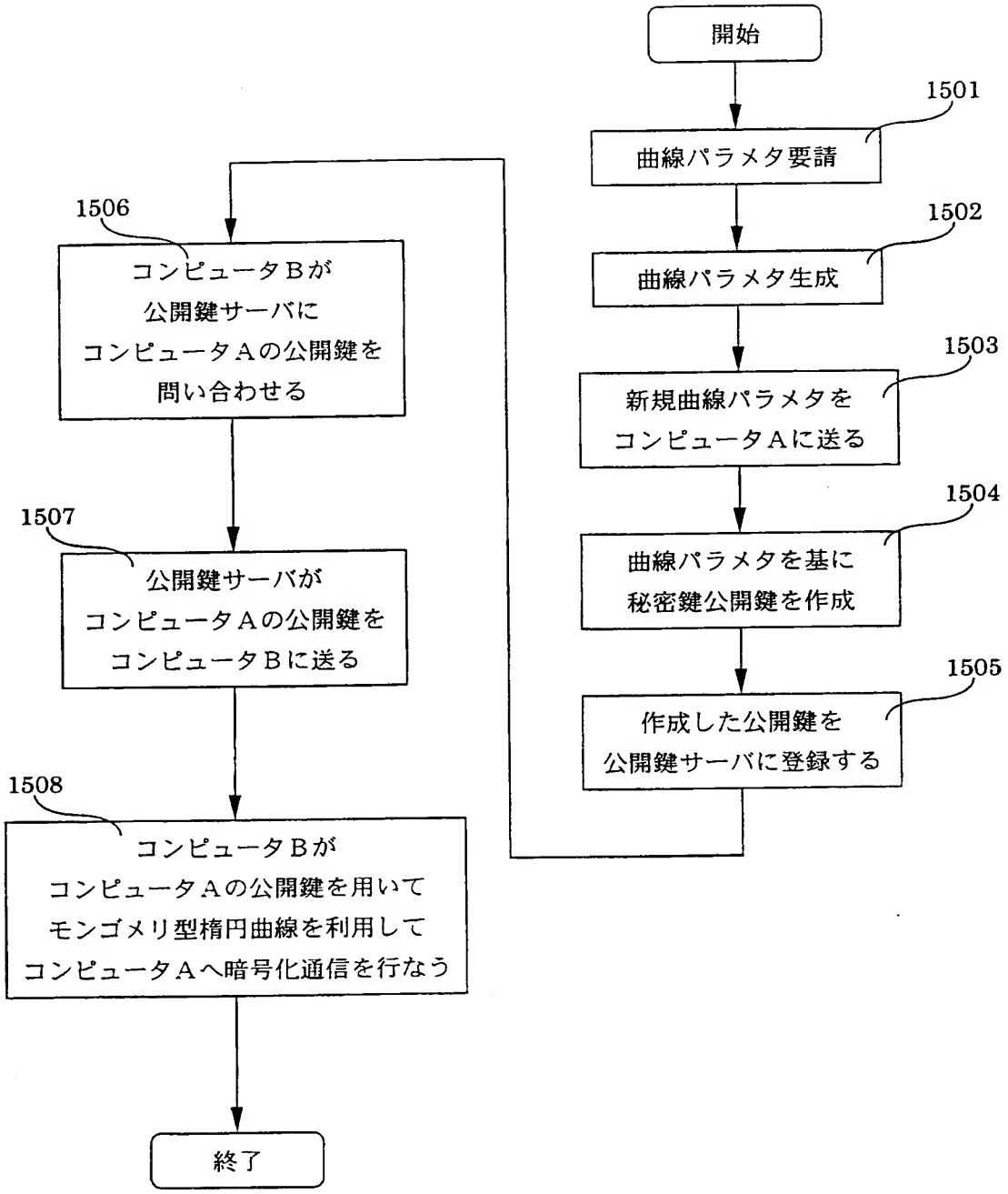
第 13 図


B
1301
0、3個
$f(x)=0$の根の数
1個
1302
平方非剰余
$f'(\alpha)$
は平方剰余
平方剰余
1303
平方剰余
$A+2$
は平方剰余
平方非剰余
1209
不適当
1305
オリジナル、
ツイスト共に選択
終了

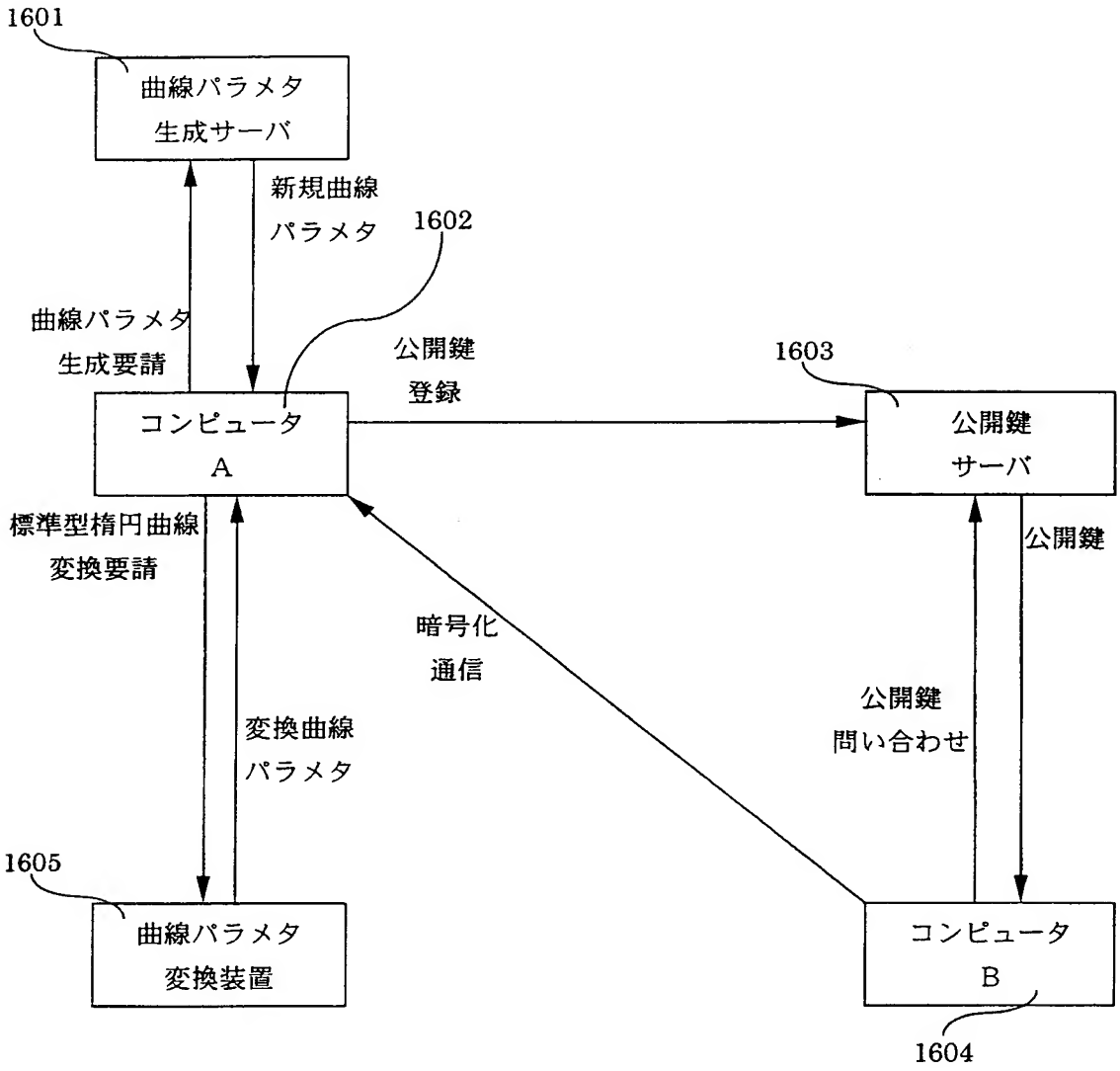
第 14 図


1401
曲線パラメタ
生成サーバ
1403
公開鍵サーバ
新規曲線
パラメタ
公開鍵
登録
公開鍵
曲線パラメタ
生成要請
公開鍵
問い合わせ
コンピュータA
コンピュータB
暗号化通信
1402
1404

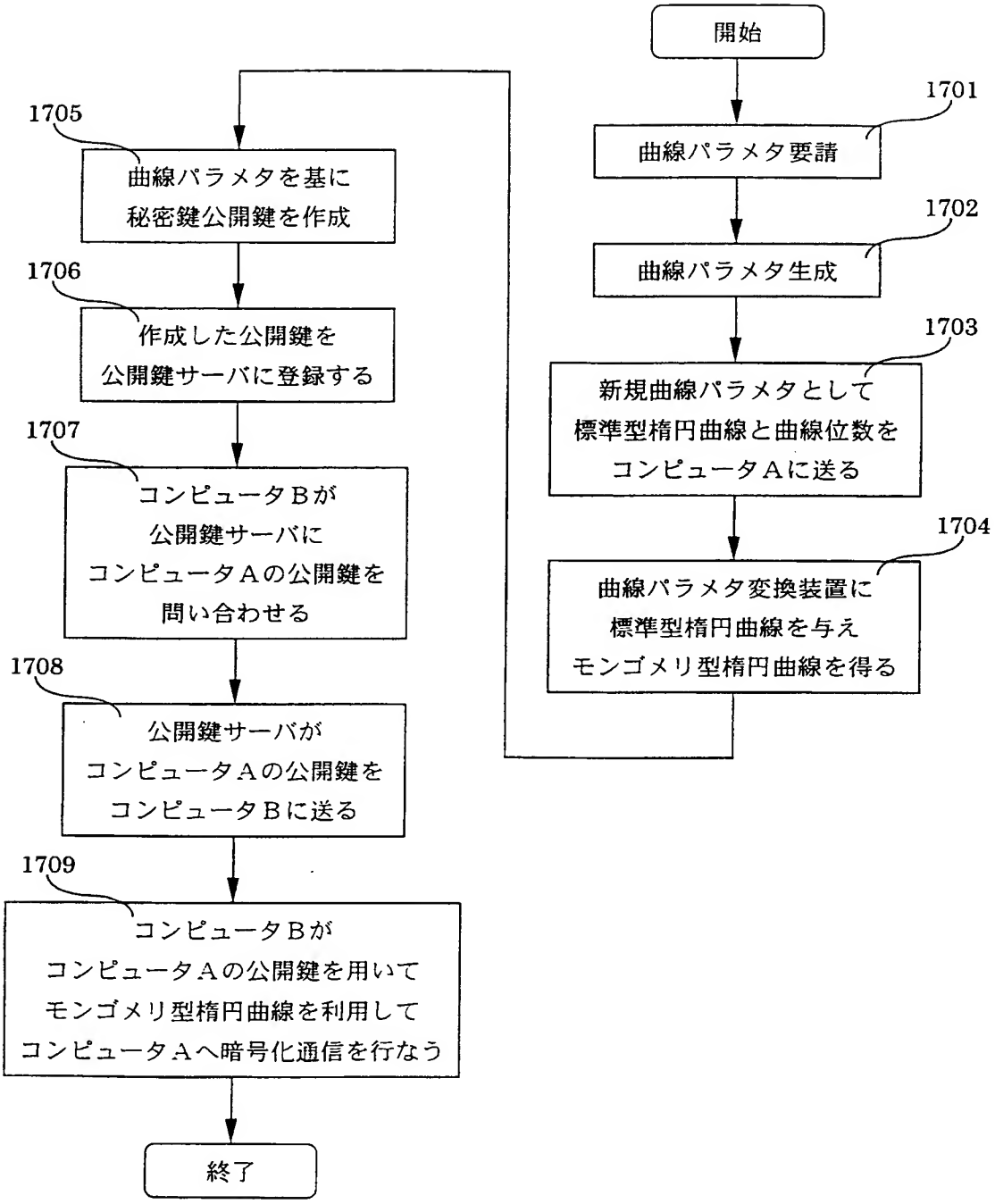
第 15 図


開始
1501
曲線パラメタ要請
1502
曲線パラメタ生成
1503
新規曲線パラメタを
コンピュータＡに送る
1504
曲線パラメタを基に
秘密鍵公開鍵を作成
1505
作成した公開鍵を
公開鍵サーバに登録する
1506
コンピュータＢが
公開鍵サーバに
コンピュータＡの公開鍵を
問い合わせる
1507
公開鍵サーバが
コンピュータＡの公開鍵を
コンピュータＢに送る
1508
コンピュータＢが
コンピュータＡの公開鍵を用いて
モンゴメリ型楕円曲線を利用して
コンピュータＡへ暗号化通信を行なう
終了

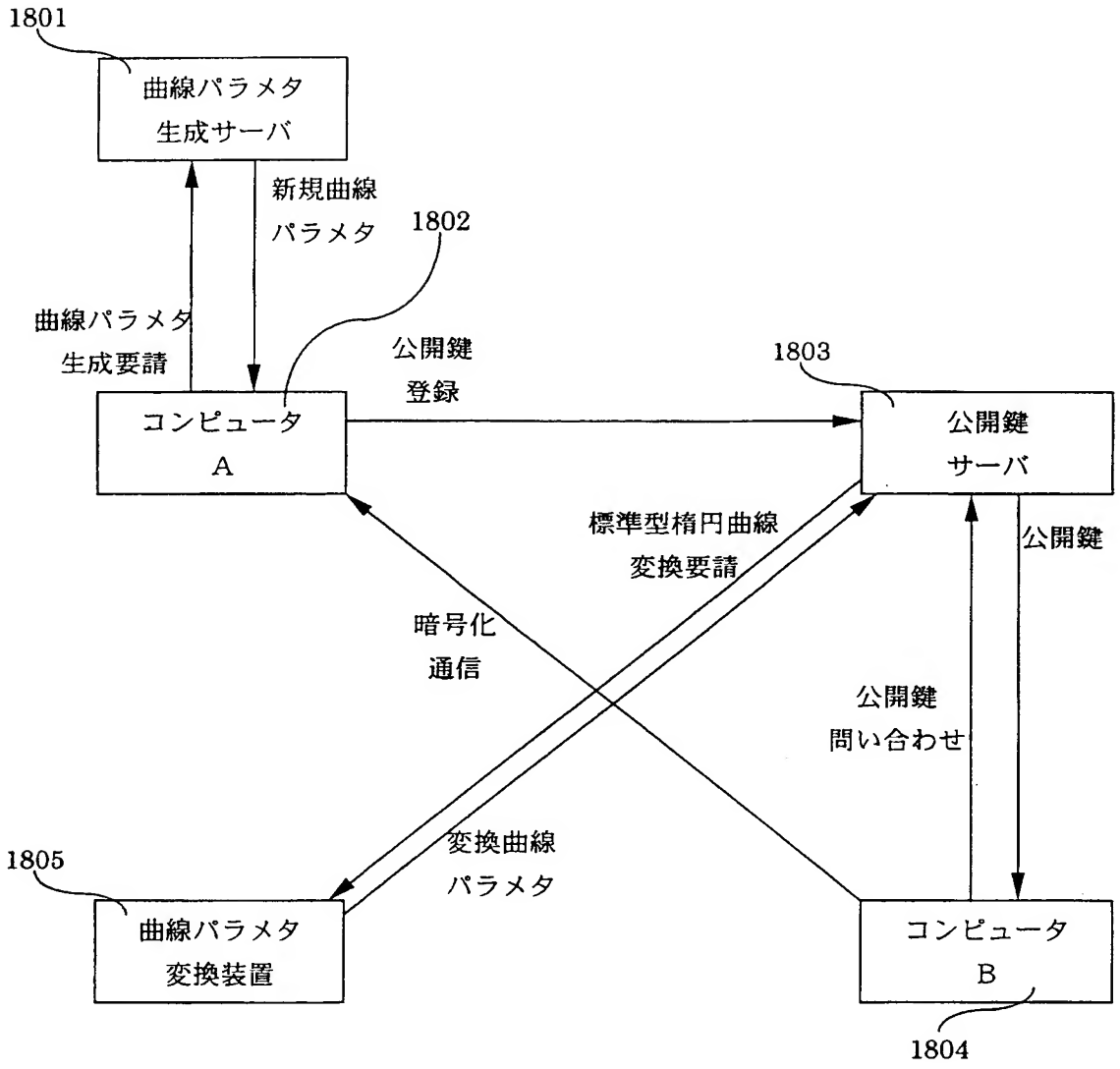
第 16 図


1601
曲線パラメタ
生成サーバ
新規曲線
パラメタ
1602
曲線パラメタ
生成要請
公開鍵
登録
1603
コンピュータ
A
公開鍵
サーバ
標準型楕円曲線
変換要請
公開鍵
暗号化
通信
公開鍵
問い合わせ
変換曲線
パラメタ
1605
曲線パラメタ
変換装置
コンピュータ
B
1604

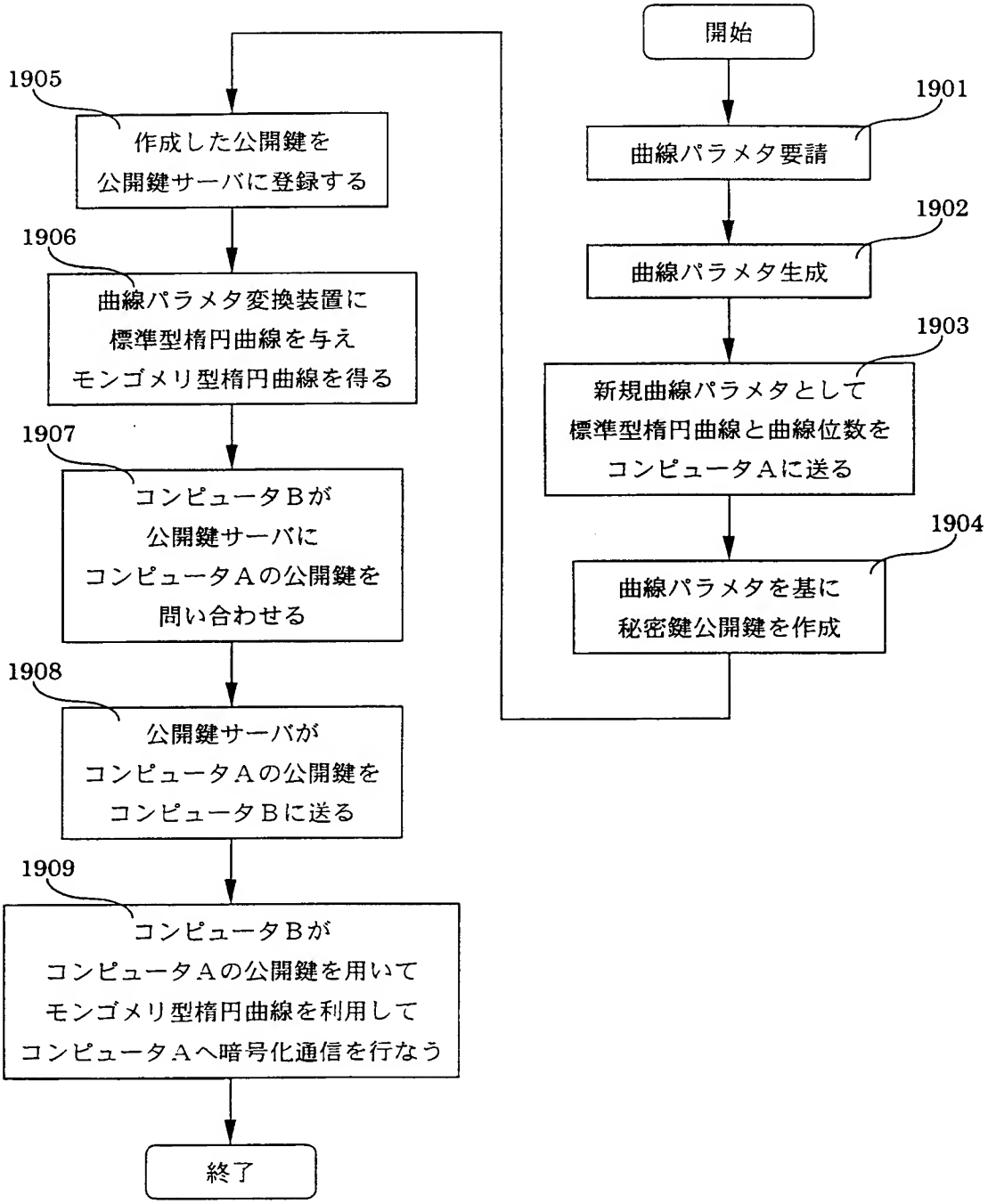
第 17 図


開始
1701
曲線パラメタ要請
1702
曲線パラメタ生成
1703
新規曲線パラメタとして
標準型楕円曲線と曲線位数を
コンピュータＡに送る
1704
曲線パラメタ変換装置に
標準型楕円曲線を与え
モンゴメリ型楕円曲線を得る
1705
曲線パラメタを基に
秘密鍵公開鍵を作成
1706
作成した公開鍵を
公開鍵サーバに登録する
1707
コンピュータＢが
公開鍵サーバに
コンピュータＡの公開鍵を
問い合わせる
1708
公開鍵サーバが
コンピュータＡの公開鍵を
コンピュータＢに送る
1709
コンピュータＢが
コンピュータＡの公開鍵を用いて
モンゴメリ型楕円曲線を利用して
コンピュータＡへ暗号化通信を行なう
終了

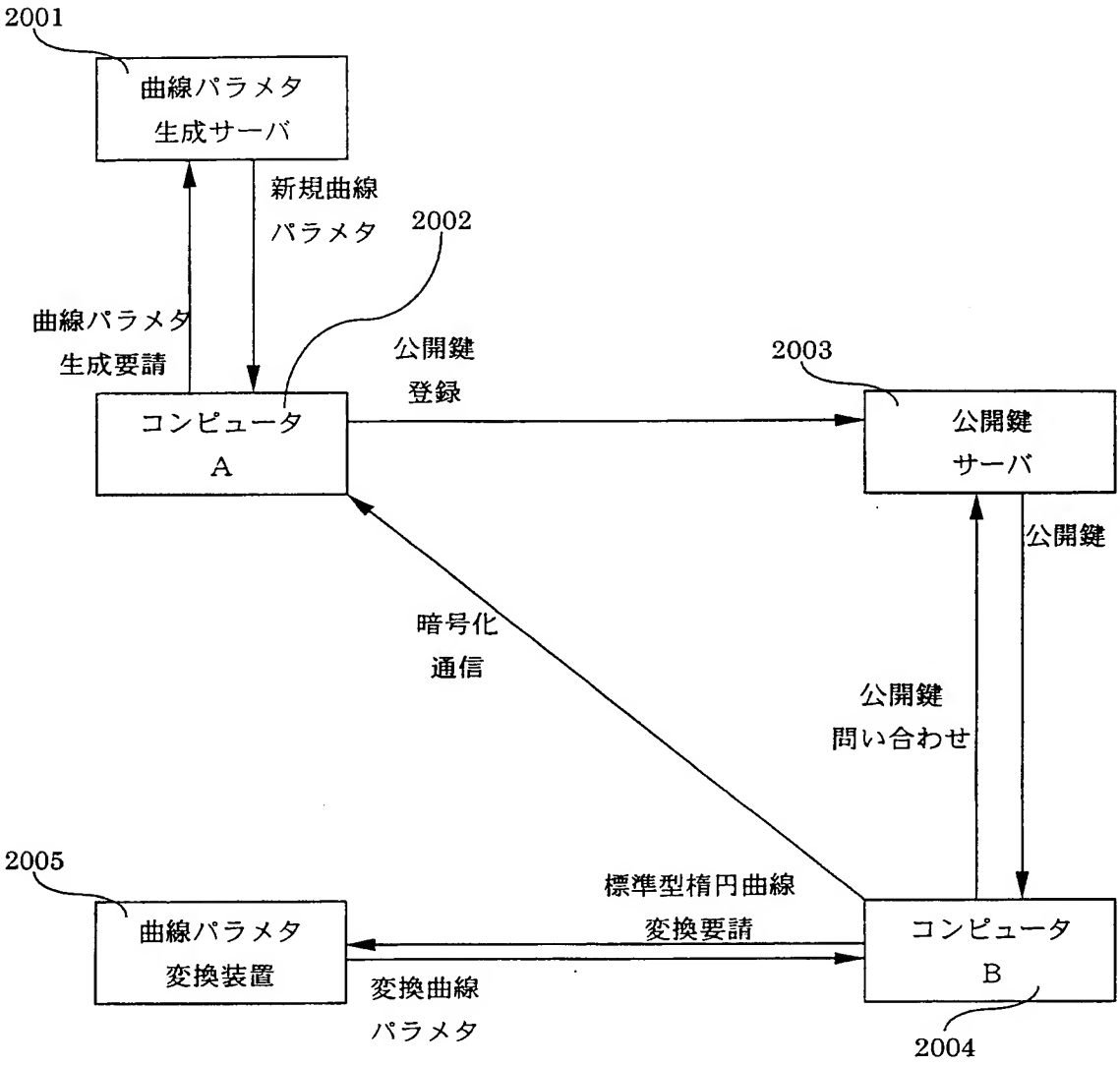
第 18 図


1801
曲線パラメタ
生成サーバ
新規曲線
パラメタ
1802
曲線パラメタ
生成要請
公開鍵
登録
1803
コンピュータ
A
公開鍵
サーバ
標準型楕円曲線
変換要請
公開鍵
暗号化
通信
公開鍵
問い合わせ
変換曲線
パラメタ
1805
曲線パラメタ
変換装置
コンピュータ
B
1804

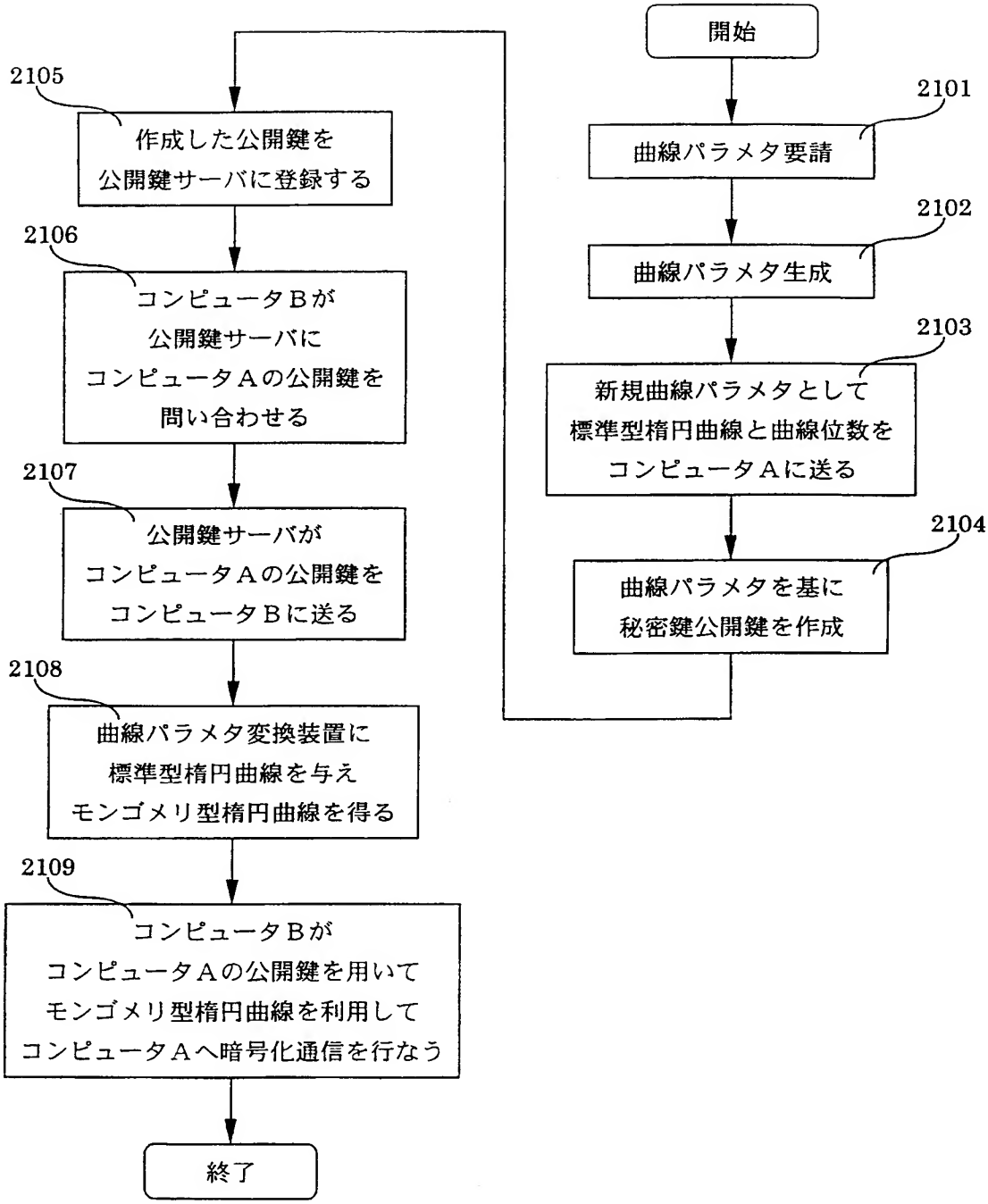
第 19 図


開始
1901
曲線パラメタ要請
1902
曲線パラメタ生成
1903
新規曲線パラメタとして
標準型楕円曲線と曲線位数を
コンピュータＡに送る
1904
曲線パラメタを基に
秘密鍵公開鍵を作成
1905
作成した公開鍵を
公開鍵サーバに登録する
1906
曲線パラメタ変換装置に
標準型楕円曲線を与え
モンゴメリ型楕円曲線を得る
1907
コンピュータＢが
公開鍵サーバに
コンピュータＡの公開鍵を
問い合わせる
1908
公開鍵サーバが
コンピュータＡの公開鍵を
コンピュータＢに送る
1909
コンピュータＢが
コンピュータＡの公開鍵を用いて
モンゴメリ型楕円曲線を利用して
コンピュータＡへ暗号化通信を行なう
終了

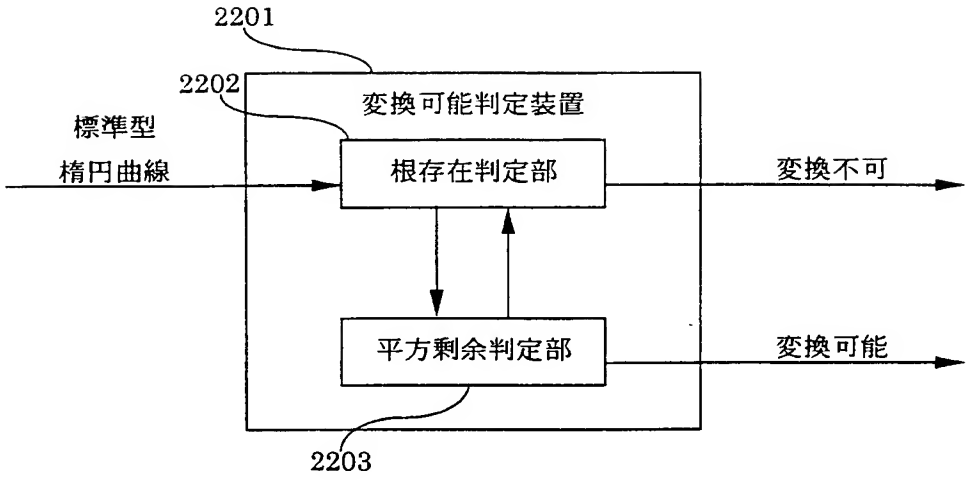
第 20 図


2001
曲線パラメタ
生成サーバ
新規曲線
パラメタ
2002
曲線パラメタ
生成要請
公開鍵
登録
2003
コンピュータ
A
公開鍵
サーバ
公開鍵
暗号化
通信
公開鍵
問い合わせ
2005
標準型楕円曲線
変換要請
曲線パラメタ
変換装置
コンピュータ
B
変換曲線
パラメタ
2004

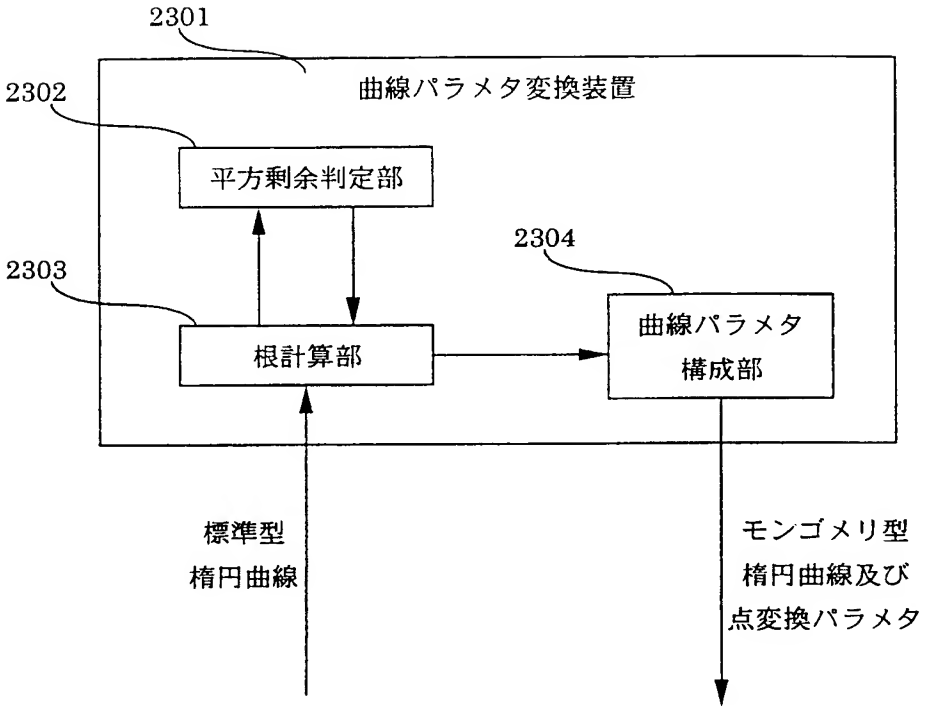
第 21 図


開始
2101
曲線パラメタ要請
2102
曲線パラメタ生成
2103
新規曲線パラメタとして
標準型楕円曲線と曲線位数を
コンピュータＡに送る
2104
曲線パラメタを基に
秘密鍵公開鍵を作成
2105
作成した公開鍵を
公開鍵サーバに登録する
2106
コンピュータＢが
公開鍵サーバに
コンピュータＡの公開鍵を
問い合わせる
2107
公開鍵サーバが
コンピュータＡの公開鍵を
コンピュータＢに送る
2108
曲線パラメタ変換装置に
標準型楕円曲線を与え
モンゴメリ型楕円曲線を得る
2109
コンピュータＢが
コンピュータＡの公開鍵を用いて
モンゴメリ型楕円曲線を利用して
コンピュータＡへ暗号化通信を行なう
終了

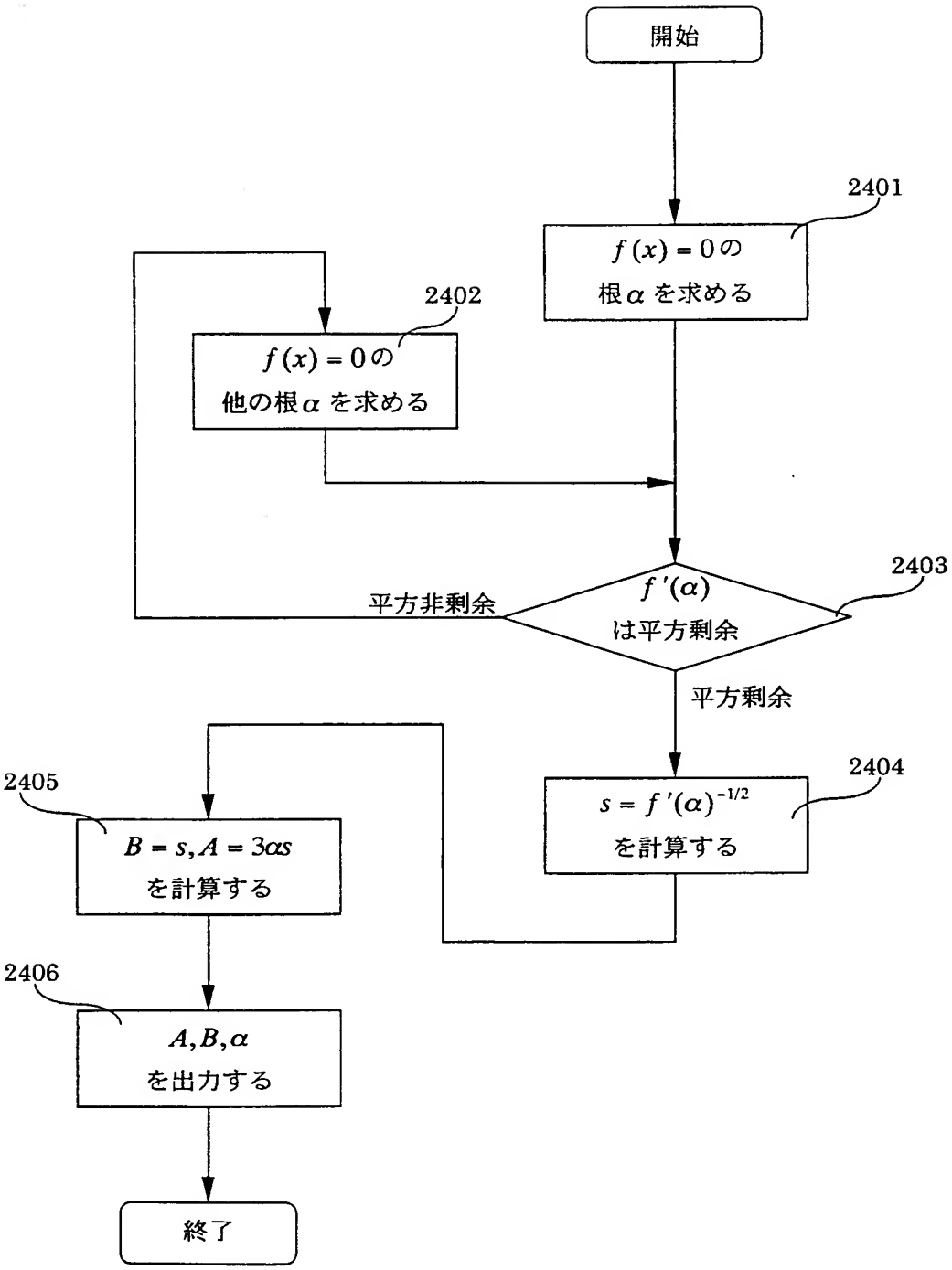
第 22 図



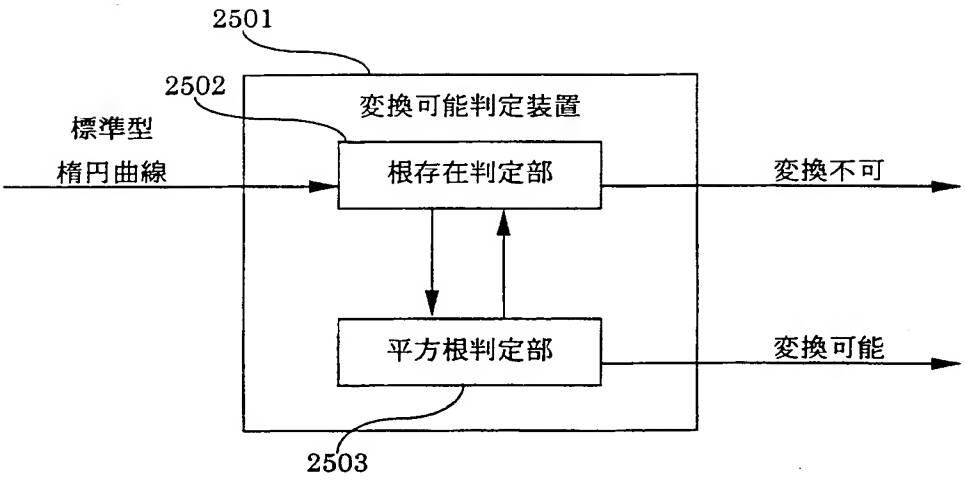
第 23 図


2301
曲線パラメタ変換装置
2302
平方剰余判定部
2303
根計算部
2304
曲線パラメタ
構成部
標準型
楕円曲線
モンゴメリ型
楕円曲線及び
点変換パラメタ

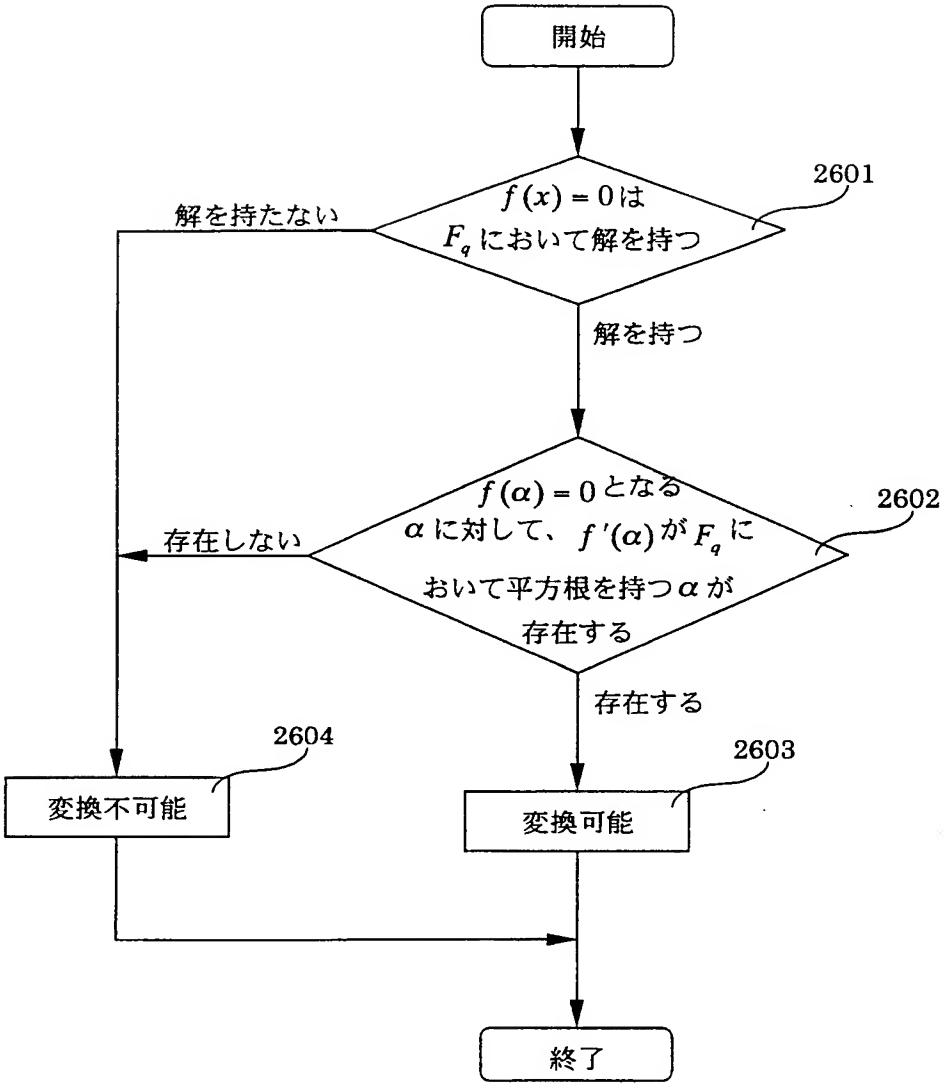
第 24 図


開始
2401
$f(x)=0$の
根$\alpha$を求める
2402
$f(x)=0$の
他の根$\alpha$を求める
2403
$f'(\alpha)$
は平方剰余
平方非剰余
平方剰余
2404
$s=f'(\alpha)^{-1/2}$
を計算する
2405
$B=s, A=3\alpha s$
を計算する
2406
$A, B, \alpha$
を出力する
終了

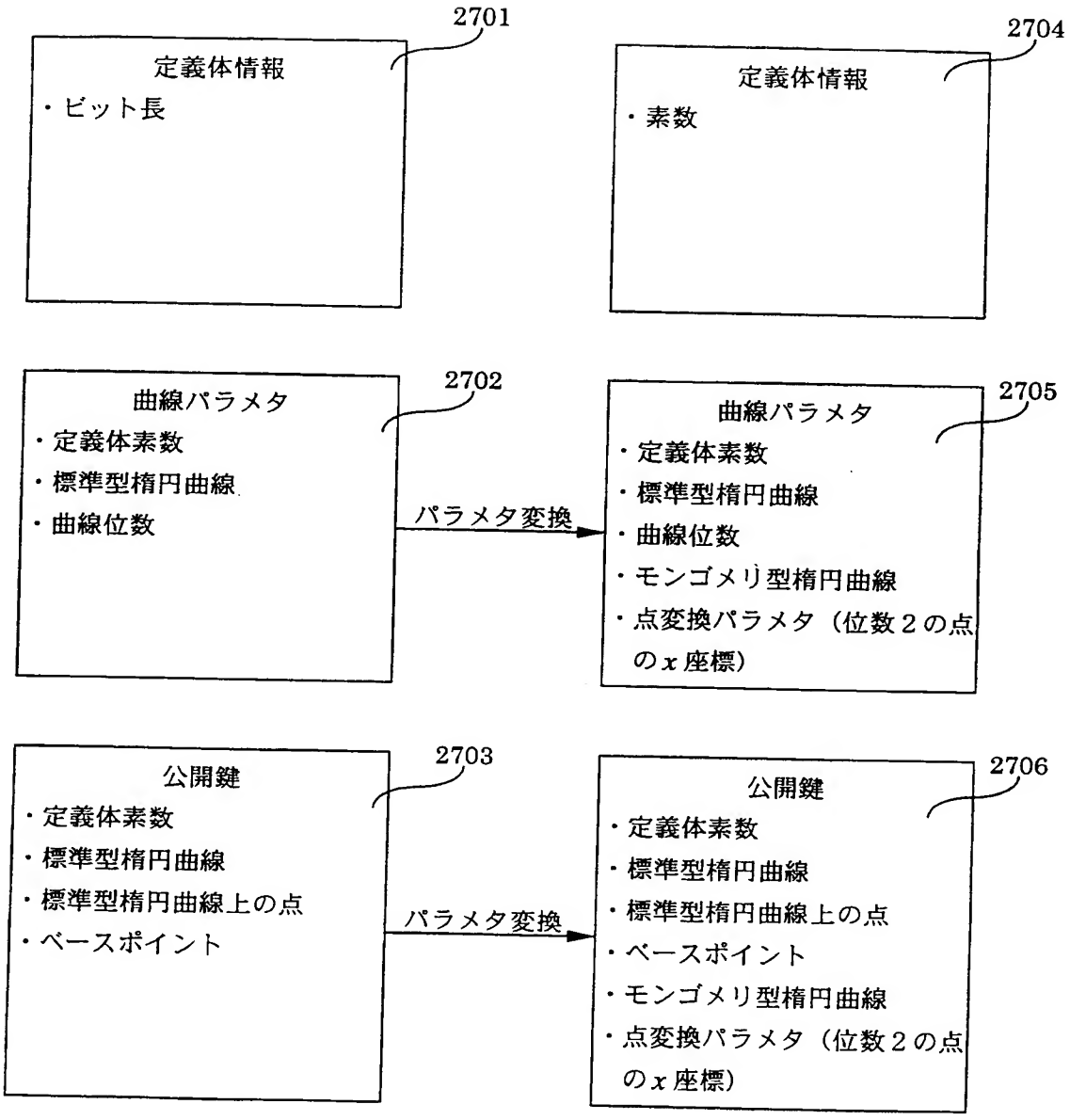
第 25 図



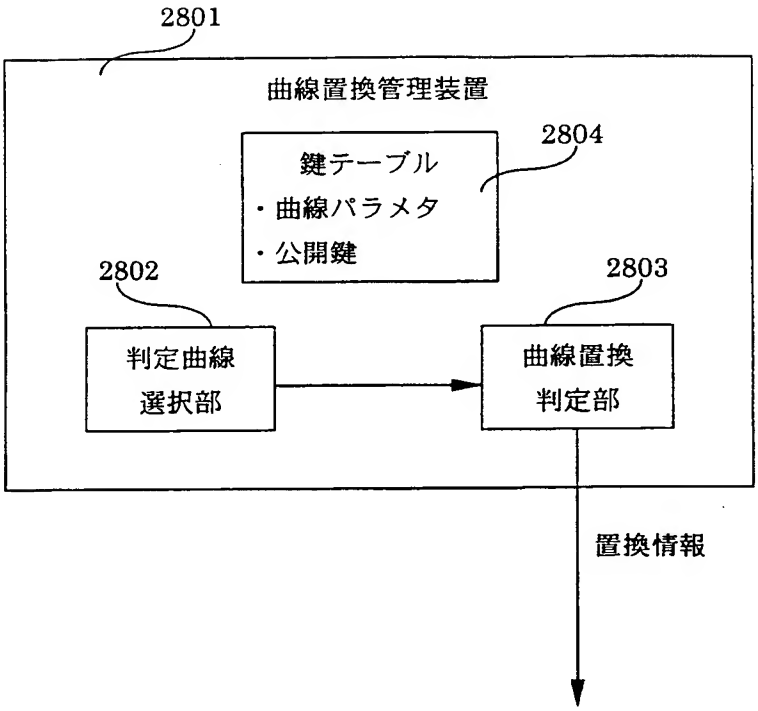
第 26 図


開始
$f(x)=0$は
$F_q$において解を持つ
2601
解を持たない
解を持つ
$f(\alpha)=0$となる
$\alpha$に対して、$f'(\alpha)$が$F_q$に
おいて平方根を持つ$\alpha$が
存在する
2602
存在しない
存在する
2604
変換不可能
2603
変換可能
終了

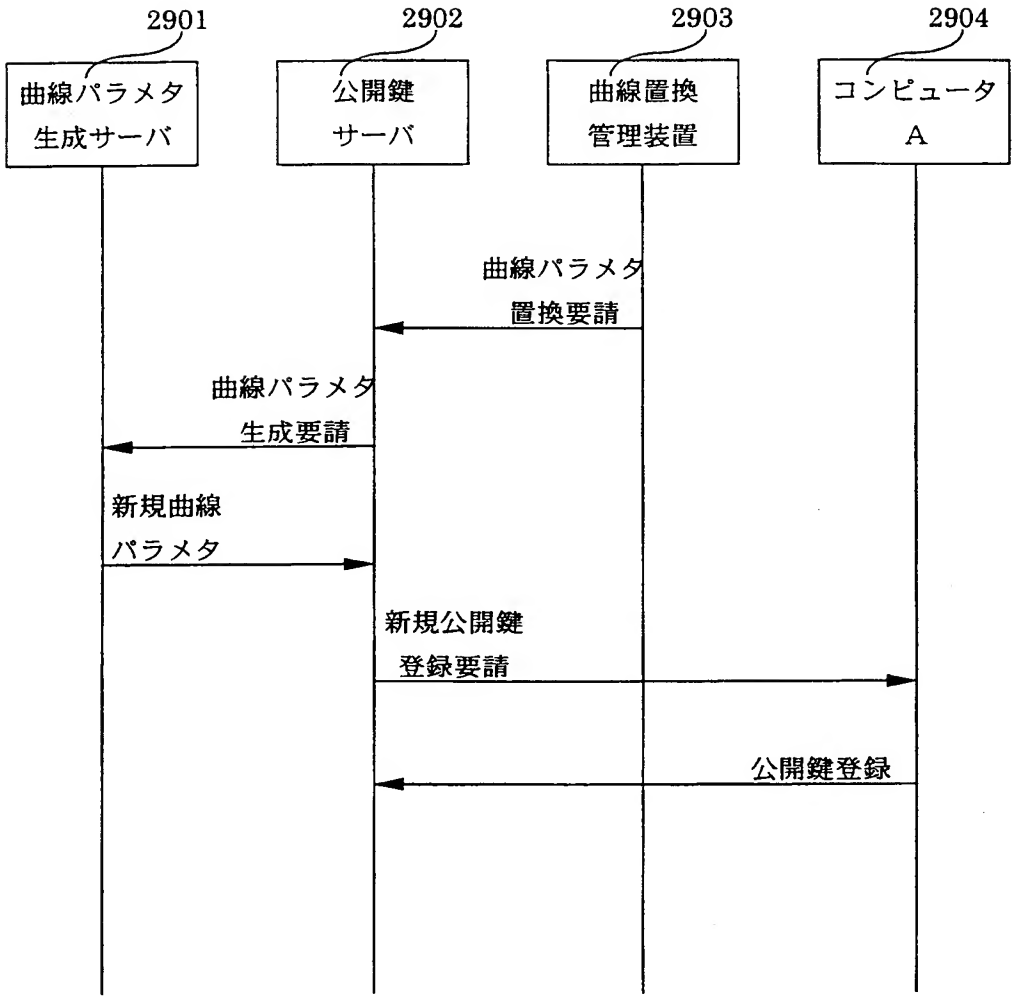
第 27 図


2701
定義体情報
・ビット長
2704
定義体情報
・素数
2702
曲線パラメタ
・定義体素数
・標準型楕円曲線
・曲線位数
パラメタ変換
2705
曲線パラメタ
・定義体素数
・標準型楕円曲線
・曲線位数
・モンゴメリ型楕円曲線
・点変換パラメタ（位数２の点のｘ座標）
2703
公開鍵
・定義体素数
・標準型楕円曲線
・標準型楕円曲線上の点
・ベースポイント
パラメタ変換
2706
公開鍵
・定義体素数
・標準型楕円曲線
・標準型楕円曲線上の点
・ベースポイント
・モンゴメリ型楕円曲線
・点変換パラメタ（位数２の点のｘ座標）

第 28 図


2801
曲線置換管理装置
鍵テーブル
・曲線パラメタ
・公開鍵
2804
2802
判定曲線
選択部
2803
曲線置換
判定部
置換情報

第 29 図


2901
2902
2903
2904
曲線パラメタ
生成サーバ
公開鍵
サーバ
曲線置換
管理装置
コンピュータ
A
曲線パラメタ
置換要請
曲線パラメタ
生成要請
新規曲線
パラメタ
新規公開鍵
登録要請
公開鍵登録

# INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP99/04869

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[6] G09C 1/00
H04L 9/30

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[6] G09C 1/00 - 5/00, H04K 1/00 - 3/00,
H04L 9/00 - 9/38

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
JICST FILE(JOIS)
INSPEC(DIALOG)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| X<br>Y<br>A | Tetsuya IZU, "Daen Kyokusen Angou Enzan no Keisanhou ni tsuite", 1999 nen Angou to Joho Security Symposium Yokoushuu, (26 January, 1999), pp.275-280 | 12, 14, 15<br>9<br>10, 11 |
| X<br>Y<br>A | Tetsuya IZU, "y Zahyou wo mochiinai Daen Kyokusen Enzan ni tsuite", Technical Research Report, the Institute of Electronics, Information and Communication Engineers, Vol.98, No.657, (10 March, 1999), pp.93-98 (SST98-129) | 12, 14, 15<br>9<br>10, 11 |
| Y | Kouichiro Akiyama, "Kakuteiteki Sosuu Hantei wo mochiita Daen Kyokusen Angou no Kagi Seisei", 1999 nen Angou to Joho Security Symposium Yokoushuu, (26 January, 1999), pp.773-778 | 9 |
| Y | Tetsuya IZU, et al., "Anzenna Daen Kyokusen Angou Parameter Sekkei (Hyousuu 2no bawai)", 1999 nen Angou to Joho Security Symposium Yokoushuu, (26 January, 1999), pp.779-784 | 9 |
| Y | Keiji Horiuchi, et al., "Daen Kyokusen no Kousei to sono Keisanryou Hyouka ni tsuite", Technical Research Report, the Institute of Electronics, Information and Communication Engineers, Vol.98, No.228, | 9 |

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

| Date of the actual completion of the international search | Date of mailing of the international search report |
|---|---|
| 07 December, 1999 (07.12.99) | 21 December, 1999 (21.12.99) |
| Name and mailing address of the ISA/<br>Japanese Patent Office<br><br>Facsimile No. | Authorized officer<br><br>Telephone No. |

Form PCT/ISA/210 (second sheet) (July 1992)

# INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP99/04869

**Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)**

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☒ Claims Nos.: 1-8,13
because they relate to subject matter not required to be searched by this Authority, namely:

Since subject matters in claims 1 to 8, 13 relate to merely mathematical theories or computer programs involving the conversion of an elliptic curve and the features of an elliptic curve, no international search is required.

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

**Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)**

This International Searching Authority found multiple inventions in this international application, as follows:

Subject matters in claims 9, 10 and 11 relate to an elliptic curve generating device which is used to generate an elliptic curve satisfying preset conditions.

Whereas, subject matters in claims 12, 14 and 15 relate to a so-called elliptic encryption; since an elliptic curve used in the encryption is a standard elliptic curve convertible into a Montgomery elliptic curve but a standard elliptic curve capable of such conversion is still at a prior art level, the subject elliptic curve constitute no special technical matter.

Therefore, claims 9, 10 and 11 and claims 12, 14 and 15 are not considered as satisfying a requirement of unity of invention.

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

**Remark on Protest**

☐ The additional search fees were accompanied by the applicant's protest.

☒ No protest accompanied the payment of additional search fees.

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| | (31 July, 1998), pp.31-36 (ISEC98-24) | |
| A | Kiyoshi Okishi, et al., "Daen Angou no Kousoku Shori ni kansuru 2, 3 no Kousatsu", Technucal Research Report, the Institute of Electronics, Information and Communication Engineers, Vol.98, No.228, (31 July, 1998), pp.37-42 (ISEC98-25) | 9-12, 14, 15 |
| A | Montgomery, P. L., "Speeding the Pollard and Elliptic Curve Methods of Factorization," Mathematics of Computation, Vol.48, No.177, (1987), pp.243-264 | 9-12, 14, 15 |

国際調査報告

国際出願番号　PCT／JP99／04869

A.　発明の属する分野の分類（国際特許分類（IPC））

Int.Cl[6]

G09C　1／00

H04L　9／30

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int.Cl[6]

G09C　1／00　－　5／00,　H04K　1／00　－　3／00,

H04L　9／00　－　9／38

最小限資料以外の資料で調査を行った分野に含まれるもの

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

JICSTファイル（JOIS）

INSPEC（DIALOG）

C.　関連すると認められる文献

| 引用文献のカテゴリー＊ | 引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示 | 関連する請求の範囲の番号 |
|---|---|---|
| X<br>Y<br>A | 伊豆哲也“楕円曲線暗号演算の計算法について”<br>1999年暗号と情報セキュリティシンポジウム予稿集,<br>(1999年1月26日), pp. 275－280 | 12, 14, 15<br>9<br>10, 11 |
| X<br>Y<br>A | 伊豆哲也“y座標を用いない楕円曲線演算について”<br>電子情報通信学会技術研究報告, Vol. 98, No. 657,<br>(1999年3月10日), pp. 93－98 (SST98-129) | 12, 14, 15<br>9<br>10, 11 |
| Y | 秋山浩一郎“確定的素数判定を用いた楕円曲線暗号の鍵生成”<br>1999年暗号と情報セキュリティシンポジウム予稿集,<br>(1999年1月26日), pp. 773－778 | 9 |

[x] C欄の続きにも文献が列挙されている。　[ ] パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの

「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）

「O」口頭による開示、使用、展示等に言及する文献

「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」同一パテントファミリー文献

| 国際調査を完了した日 | 国際調査報告の発送日 |
|---|---|
| 07. 12. 99 | 2.99 |

| 国際調査機関の名称及びあて先 | 特許庁審査官（権限のある職員） | |
|---|---|---|
| 日本国特許庁（ISA／JP）<br>郵便番号100－8915<br>東京都千代田区霞が関三丁目4番3号 | 丸山　高政 | 5W　9570 |
| | 電話番号　03－3581－1101　内線　3576 | |

様式PCT／ISA／210（第2ページ）（1998年7月）

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ９９／０４８６９

第Ⅰ欄　請求の範囲の一部の調査ができないときの意見（第１ページの２の続き）

法第８条第３項（ＰＣＴ１７条(2)(a)）の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1．[x] 請求の範囲　１－８，１３　は、この国際調査機関が調査をすることを要しない対象に係るものである。
つまり、
請求の範囲１－８，１３に記載されたものは、楕円曲線の変換と楕円曲線の性質に関する数学の理論又はコンピュータプログラムにすぎないものであるから、国際調査をすることを要しない。

2．[ ] 請求の範囲　＿＿＿＿＿＿＿＿　は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、

3．[ ] 請求の範囲　＿＿＿＿＿＿＿＿　は、従属請求の範囲であってＰＣＴ規則6.4(a)の第２文及び第３文の規定に従って記載されていない。

第Ⅱ欄　発明の単一性が欠如しているときの意見（第１ページの３の続き）

次に述べるようにこの国際出願に二以上の発明があるとこの国際調査機関は認めた。

請求の範囲９、１０及び１１は、楕円曲線生成装置に関するものであり、所定の条件を満たす楕円曲線を生成するためのものである。
一方、請求の範囲１２，１４及び１５は、いわゆる楕円暗号に関するものであり、そこで使用される楕円曲線はモンゴメリ型楕円曲線に変換可能な標準型楕円曲線であるが、このような変換が可能な標準型楕円曲線は先行技術の域をでないから、この楕円曲線は特別な技術的事項ではない。
したがって、請求の範囲９．１０及び１１と請求の範囲１２，１４及び１５は単一性の用件を満たしているとは認められない。

1．[x] 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。

2．[ ] 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。

3．[ ] 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったので、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。

4．[ ] 出願人が必要な追加調査手数料を期間内に納付しなかったので、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

追加調査手数料の異議の申立てに関する注意
[ ] 追加調査手数料の納付と共に出願人から異議申立てがあった。
[x] 追加調査手数料の納付と共に出願人から異議申立てがなかった。

| 国際調査報告 | 国際出願番号　ＰＣＴ／ＪＰ９９／０４８６９ |
|---|---|

C（続き）．　関連すると認められる文献

| 引用文献のカテゴリー＊ | 引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示 | 関連する請求の範囲の番号 |
|---|---|---|
| Y | 伊豆哲也，小暮淳，野呂正行，横山和弘<br>“安全な楕円曲線暗号パラメータ設計（標数２の場合）”<br>1999年暗号と情報セキュリティシンポジウム予稿集，<br>(1999年1月26日)，pp. 779－784 | 9 |
| Y | 堀内啓次，布田裕一，境隆一，笠原正雄<br>“楕円曲線の構成とその計算量評価について”<br>電子情報通信学会技術研究報告，Vol. 98，No. 228，<br>(1998年7月31日)，pp. 31－36（ISEC98-24） | 9 |
| A | 大岸聖史，境隆一，笠原正雄<br>“楕円暗号の高速処理に関する二，三の考察”<br>電子情報通信学会技術研究報告，Vol. 98，No. 228，<br>(1998年7月31日)，pp. 37－42（ISEC98-25） | 9-12，14，15 |
| A | Montgomery，P. L.，<br>“Speeding the Pollard and Elliptic Curve Methods of Factorization，”<br>Mathematics of Computation，Vol. 48，No. 177，(1987)，<br>pp. 243－264 | 9-12，14，15 |